GIRITECH®

Version

3.6

G/On™ Installation Guide & Admin Manual

GIRITECH A/S

G/On Installation Guide & Admin Manual

© Giritech A/S, 2009
Herstedøstervej 27-29 • C2
2620 Albertslund
Denmark
Phone +45 70.277.262

Legal Notice

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks and registered trademarks of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property currently includes the patented systems and methods known as EMCADS™. Other product names and brands used herein are the sole property of their owners. Unauthorized copying, editing, and distribution of this document is prohibited.

Table of Contents

Introduction 5
Who is this Guide For? 5
How the Manual is Organized 5
Support 5
Understanding G/On 6
G/On Server 6
G/On Client 7
Overview of G/On Configuration & Deployment 9
Configuration & Requirements for Your Environment 10
G/On Server Requirements 10
Bandwidth Considerations 11
Where to Place your G/On Server 11
Firewall Configuration 12
Failover Configuration & Setup 13
Directory Synchronization 14
Client Requirements 14
DNS Settings 16
Anti-Virus Settings – Server side 16
Database Setup 16
Using Virtual Servers 17
G/On Installation & Server Configuration 18
Installing G/On 18
G/On Builder 23
G/On Server Settings and License Activation 24
Advanced Server Settings 25
Enabling different admin application passwords 27
User Directory and Database Configuration 27
Validation Settings 29
Client Update Folder Settings 31
AD Sync 32
Clients 34
Completing and Activating the G/On Server 37
Moving G/On to another server. 38

Installing multiple G/On servers. 39
Upgrading G/On 41
Prior to Upgrade 41
Installing the Upgrade 42
G/On Builder Changes during Upgrade 43
Upgrading your Clients to the Latest Version....44
Migrating to an External Database[EP] like MS SQL Database 45
Changes to Zone Rules for USB Keys (pre-3.3) 46
Zone Configuration with the G/On AccessRules Manager.... 47
Zone Types....48
Setting up Zones 49
Add or Manage Zones....50
Defining Your Own Zones 50
Examples of Zones:....51
Important Changes to Zone Rules for USB Keys when upgrading from pre-3.3 G/On 53
Assigning Zones to Groups....54
Manage EDCs 55
G/On Admin.... 56
Getting Started as an Administrator 58
Defining Administrator Levels in G/On Admin....58
Administrator Access Overview....59
File Menu....60
Synchronize Active Directory 60
Running USync 61
Running AdSync....62
Overview of G/On Application Connectivity 72
Advanced Application Connectivity: What is a String 72
Four Step Method for Defining and Configuring Applications 73
Defining Application Strings and Menu Actions 74
Application Connectivity Settings Overview....79
Creating Menus 85
Groups Tab....87
Creating Local Groups 88
Assigning Groups to Zones....89
User Administration 90
Adding Users....91
Assigning/Changing a Users Group Association: 92
Selecting/Searching Users....93
Activating/ Enabling Users 94
Enabling Locked Out Users....94
Deleting Users....95

Copyright Giritech A/S 2009

Viewing Online Users 95
Disconnecting Users 95
Adopting Users 96
What is being Adopted 96
Why Adoption is Important 97
G/On Builder Settings for Adoption 98
Adopt EDC from File 98
Manually Adopting EDCs 99
Assigning/Locking EDCs 99
Distributing & Deploying Clients 100
Best Practice Distribution Methods 100
Distribution Methods Step by Step 101
Deploying Clients with G/Update 103
Deploying G/On USB Clients 104
Deploying Desktop Clients 104
Instructing Users to Deploy Keys 105
Notes on G/On Desktop Adoption 106
G/On Desktop Users Upgrading from G/On 3.5 or previous version. 106
Upgrading Clients 107
How G/Update works on Upgrades 107
Automating update of the Clients and the Applications after upgrade 108
Automatically Update Clients Read/Only Partition 109
Manually Update Clients Read/Write Partition 112
Creating an Update Menu Item: 112
Instructing Users to Manually Update their Clients 112
System Backup & Restore 117
Signing Keypair Backup 117
G/On Backup /Restore 118
G/On Restore 118
Overview of Application Connectivity 119
Introduction to HTTP proxy support 122
Introduction to the HTTP proxy tool 122
Compliance and tested proxies 129

Copyright Giritech A/S 2009

Introduction

The *G/On Installation Guide and Admin Manual* is a concise usable resource for Certified G/On Partners and G/On Administrators.

This Manual covers everything you need to initially install, upgrade, administrate and configure applications for your Giritech G/On solution.

Who is this Guide For?

The *G/On Installation Guide and Admin Manual* is designed for:

Technical personnel with a basic understanding of TCP/IP based networks, firewalls and services.

Accomplished Administrators who have experience installing, configuring and administrating Microsoft Windows servers.

System Administrators with a fundamental understanding of Microsoft Active Directory.

How the Manual is Organized

G/On Installation Guide and Admin Manual is to be used in the implementation, upgrade and routine administration of your G/On installation.

☑ Network, Firewall and Database Pre-configuration: Chapter 2

☑ System Configuration, Zone Setup and Application Connectivity: Chapters 3-6

☑ Routine Administration, User synchronization and Client Deployment: Chapters 7-11

Note: *this manual covers all versions of G/On (Enterprise and Business). Functionality that is only included in G/On Enterprise (but optionally in G/On Business) is marked with an* EP *mark. Functionality marked* Option *is optionally for both versions.*

All screenshots in this manual are either Windows Server 2003 or Vista – but the contents of the screens are exactly the same across all versions of supported operating systems.

Support

Every effort has been made to ensure the accuracy of the contents of this manual. Any corrections will be posted to the latest online *G/On Installation Guide and Admin Manual* at the Giritech Website (www.giritech.com) under *Support*.

If you require additional support or further assistance, please contact Giritech Support at: support@giritech.com.

Copyright Giritech A/S 2009

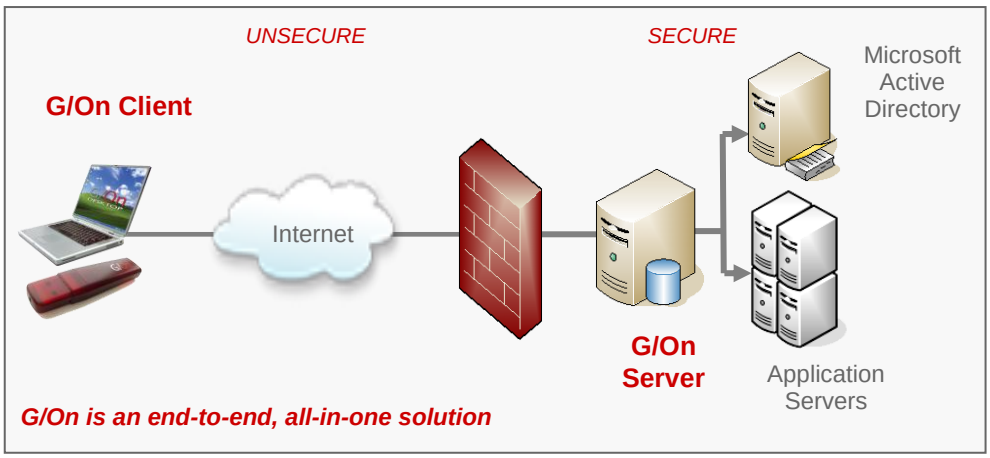
Understanding G/On

G/On gives IT professionals the ability to securely extend internal applications to users, partners, vendors, external contractors and others in a way that is easy to administrate. User and group information can be synchronized with domains[1] in Microsoft AD, allowing for easy configuration of menus.

The G/On product consists of two primary parts:

G/On Server

G/On Client



G/On Server

The G/On Server is a Windows Based Server Application, based on Giritech's EMCADS™, Encrypted Multipurpose Content and Applications Deployment System) technology. The EMCADS™ Data Management System (EDMS) is used for storing and accessing information about applications, users, groups, adopted keys, rules, zones and access statistics.

The G/On Server has one TCP port open for incoming connections and forwards the relevant parts of incoming connections to services on the network it is attached to. This only occurs once a connection has been established.

The G/On Client (either G/On USB or G/On Desktop) first verifies that it is connecting with the right server using a signing key-pair. The G/On Server then verifies that the G/On Client belongs to the system. This verification is done by means of a unique serial number that unambiguously identifies the actual device, referred to as the EDC, Electronic Data Carrier (e.g. USB key or host PC). It then checks for connection rules, allowing or denying access to that client.

The Client is assigned into one or more zone(s) that reflects the defined level of trust versus access that has been set by the systems administrator during the installation.

---

[1] EP:Synchronization with *multiple* domains in complex AD structures are only supported in G/On Enterprise

Copyright Giritech A/S 2009

Once the Server has verified the client and assigned the appropriate zone, the G/On Server authenticates the user, either against the AD or the EDMS. The AD is not queried until the G/On Server verifies that the user exists in the EDMS.

The AD is never exposed, and the AD passwords are never stored in the EDMS.

Finally, once the User has been authenticated the Server presents a menu to the client. Menus are dynamic and the menu presented to the user is defined by the administrator and can vary based on user name, user group associations, and access zones.

G/On Client

The G/On Client is currently either a G/On USB Key or a G/On Desktop client.

Two-factor authentication is implemented using 163 bit Elliptic Curve Cryptography (ECC), a standards-based, public key technology, to generate key pairs, which are used for encrypting and signing the initial handshake prior to user logon.

By verifying the server's digital signature, created with the ECC key, the client is also validating the server, before any connection continues.

Once the handshake is completed, all data is encrypted using 256 bit Advanced Encryption Standard (AES). Each new application session goes through the handshaking procedure, establishing a new AES encrypted connection. This means that all application sessions run on individual connections, preventing data leaks between sessions. As an added security precaution, two separate AES key pairs are used, one for upstream traffic and one for downstream traffic.

Any tampering with a connection will cause the application session to be disconnected by the G/On Server, but will not influence other application sessions. The client opens ports on the client PC's local loopback interface (127.0.0.2) and forwards communication to and from this port through the G/On Server. A technique called LockToProcess prevents any other application from using the session to access the intranet. Only the proper application will be allowed to connect through the loopback interface.

Warning:

G/On release 3.6 uses a new EDC detection routine for identifying the computers from which access is given. This means that *all* desktop clients adopted with G/On version 3.5 or older will have to be re-adopted after installation of G/On 3.6. PLEASE SEE Notes on G/On Desktop Adoption on Page 106 before deploying the new G/On Desktop Clients.

Copyright Giritech A/S 2009

Chapter 1

Overview of G/On Configuration & Deployment

From beginning to end there are 6 major categories you will need to complete to get up and running with your G/On Solution.

Preparation and Network Setup	Installation or Upgrade	User Setup	Administrator Setup & Configuration	Client Deployment	Administration
Bandwidth Review	Installation of the G/On Server	User Synchronization & Database Population	User Access Locations Security (Zone Setup)	Best Practice USB Key Deployment	Server Backup
Firewall Settings	Creating the Database		Application Connectivity Creation	Best Practice Desktop Client Deployment	G/On Configuration Backup
User Directory Setup	Configure User Login Security Features		Connect Applications	User Guidelines	Adding New Users
Failover Setup	Configure the Client connections		Create and Assign User Groups & Menus		Removing Users
DNS Settings	Create your Company Specific Identity File				
Database Preparation HTTP Proxy support	Activation of G/On				

Copyright Giritech A/S 2009

Chapter

2

Configuration & Requirements for Your Environment

Before you install your G/On Server, you need to prepare your network environment. This section covers the basic pre-requisites you must have to successfully install, configure and run G/On.

SECTION OVERVIEW

- ☑ Server Software and Hardware Requirements
- ☑ Bandwidth Considerations
- ☑ G/On Server Placement in the Network Environment
- ☑ Firewall Configuration
- ☑ Failover Setup & Configuration
- ☑ User Directory Setup
- ☑ Client Software & Hardware Requirements
- ☑ DNS Settings
- ☑ Database Setup & Preparation
- ☑ Use of Virtual Servers[EP]

To save time during the installation and configuration process, we process, we recommend that you make the necessary preparations preparations to your network environment prior to installation of installation of G/On.

G/On Server Requirements

Server Hardware

USB port version 1.1 or higher

Minimum two virtual drive mappings available (e.g. drives E:\ and F:\). *Optional Tokenless [Option] support available*

120 Mb of available hard disk space

Minimum 1.2GHz Processor

Minimum 512 MB memory for up to 100 concurrent users

2 GB memory for a recommended maximum of 500 concurrent users

Server Software

Your G/On Server can use one of the following:

Microsoft Windows Server 2003 SP2

Microsoft Windows Server 2003 R2 SP2 *(32 bit and 64 bit)*

Microsoft Windows Server 2008[2] *(32 bit and 64 bit)*

[2] Please note that G/On 3.6 have been tested with *basic* Windows Server 2008 functionality, only Terminal Server 2008 and Active Directory 2008 have been tested with G/On 3.6. Please contact Giritech support for latest details on Windows Server 2008 support.

Limited support for Windows Server 2000 SP4 (*please contact Giritech support for details*)

Dimensioning the Server

The G/On Server is not CPU intensive, but CPU usage will increase as the amount of concurrent users increase.

Bandwidth Considerations

Network bandwidth is a key factor and probably the primary bottleneck if not properly sized. The network and server administrators should be able to monitor bandwidth for saturation.

The available network bandwidth is halved in the case where both inbound and outbound traffic uses the same network adapter on the G/On Server.

To scale network performance, a second network adapter can be installed, assigning one to the inbound connections from the users and the other to the LAN where the application servers are located. No routing between the interfaces is needed. This configuration also provides a physical separation of “inside” and “outside” that helps increase the security level.

Where to Place your G/On Server

Physical placement for the G/On server is a business choice i.e. it depends on the level of security that the company would like to maintain. We recommend the following, in prioritized order:

Preferred Server:

1. Placement on a dedicated hardware provides the highest level of security
2. Placement on a separate virtual server (using Tokenless *Option*)
3. Proxy Server
4. Terminal Server

Not Recommended:

We do not recommend installation on other types of servers. And NEVER on the same box as the AD Server or a Web Server as this presents a grave security risk.

Placement in the Firewall/LAN Infrastructure:

The EMCADS server has been designed to be placed securely on the inside of the Firewall where the application servers are.

In this configuration only one port (default 3945 or as configured) in the Firewall will be open from the outside. All traffic on this port should be forwarded to the G/On server, and only to the G/On server. And the traffic on this port will be limited to the applications that the remote users have been authorized to access. Direct access to the infrastructure is avoided, since the user only has access to predefined applications and the remote PC is never assigned an IP address on the internal network where the G/On Server resides. All traffic running on this port is encrypted and protected.

Firewall Configuration

Configuration of your firewall impacts the:

- Activation and Upgrade of your G/On installation
- Where Clients connect during general operations
- Failover

General Firewall Requirements

The default setting for G/On communication is via the default IANA assigned port 3945. To use the default settings, configure your firewall Port 3945/tcp for Inbound Traffic.

Changing the Default Listening Port

We do not recommend changing the standard listening port (3945/tp), and instead recommend that you configure alternative external listening ports with Port Address Translation (PAT) features on your firewall. (See below)

If you for some reason still wish to change the listening port for daily operations, you can change the default listening port from Port 3945/tcp to another TCP port by changing the settings during G/On installation. If you choose to change the default port configure your firewall to pass traffic from the same port to the G/On Server.

Alternative External Listening Port Configuration with PAT

If you would like to externally listen on port(s) OTHER than 3945/tcp, you can use Port Address Translation in your Firewall's configuration to map additional ports on the outside firewall to the G/On Server. We suggest using external 3945/tcp, 443/tcp and 80/tcp which all must be PAT to 3945/tcp on the inside. *(see section on Failover with 1 IP address for more information)*

Licensing & Activation Requirements on Firewall Configuration

G/On version 3.6 support a range of license activation options. In the default setting the G/On server will contact the Giritech licensing server at `license2.giritech.com` on port 3945/tcp. *This port must be open, outbound from the G/On server during license activation and upgrades.* The port does not have to remain open during normal operation.

In case license communication fails on port 3945/tcp, the G/On server will automatically try port 443/tcp and port 80/tcp successively to see if connection to the Giritech license server can be established on one of these ports.

If all 3 ports fail due to outgoing traffic from G/On server towards the Internet being blocked, the G/On server can still be installed using the optional "*Offline license*" feature. Please contact Giritech Support for more information.

When using the "*Offline license*" feature, no changes are required to the local firewall for licensing purposes.

Copyright Giritech A/S 2009

Note:

Previous versions of G/On (3.4 and older):

Older versions of G/On communicates differently with a different Giritech licensing server at `license.giritech.com`:

G/On 3.4 uses port 80/tcp for communication with the Giritech licensing server. The firewall port 80/tcp MUST allow unrestricted outbound traffic from the G/On server.

G/On 3.3.1 and older *only* communicates with the Giritech license server on port 3945/tcp. Only exception is G/On 3.3.1 which will try to fallback to port 80/tcp in case port 3945/tcp fails.

Failover Configuration & Setup

G/On currently supports a Stateless failover method. Your G/On License must be configured for the following:

1. At least one Additional Server *Option*
2. Tokenless *Option*
3. External Database (not required, but recommended)

In terms of hardware you will need to install a second G/On server

Note that if the Tokenless *Option* option has been enabled you will not need to have the token active on the server.

Note:

Database Choice:

When implementing stateless failover please use the MS SQL Database option[EP]. This database will be less resource intensive to administrate as you can use one database for both G/On servers and you only have to maintain one database backup routine.

In order to configure your environment for Failover, please go to page 39 and follow the directions on setting up multiple G/On servers. Furthermore you have the following options available:

FAILOVER CONFIGURATION CHECKLIST

- ☑ Install the second G/On Server
- ☑ Check that the signed key pairs are identical (copy & paste)
- ☑ Check that your IP addresses are correctly entered into G/On Builder
- ☑ Verify that the listening port is correct in the Advanced settings of G/On Builder
- ☑ Verify that the firewall setup is correct, incl. ports, NAT and PAT configuration

Failover using 2 External IP Addresses

1. Request 2 unique External IP Addresses.
2. When configuring your initial G/On Server, enter both IP addresses into the Clients Tab of G/On Builder. This is done in the field “EMCADS Server DNS name or IP Address”
3. The listening port can remain 3945 for both the primary and the failover servers.
4. Copy your G/On server to the backup/failover server.

Failover Using 1 External IP Address

1. You will have to use your firewall’s Port Address Translation (PAT) features to configure the traffic from the External Port to the internal G/On Server listening ports.
2. Install your primary G/On server as normal and leave the listening port set to 3945/tcp.
3. When configuring your initial G/On Server, enter the IP address into the Clients Tab of G/On Builder. In the field “Port Connects to” on the “Clients” tab enter the Ports that you have defined in the firewall, separated by commas. ie. 3945,443.
4. Activate your Primary G/On server and generate your signing key pair.
5. Install your secondary G/On Server with all the same settings. Copy the signing keypair from your Primary server installation.
6. Define the listening port to listen to a different port, ie. 443/tcp.

Directory Synchronization

Two separate tools is provided for AD synchronization: The default USync tool for smaller installations and installations running on the internal G/On database and AdSync for larger G/On installations with more than 200 users (see later chapter on AD Sync, page 32).

For synchronization with the AD, G/On Server must be a full member of the Domain.

If you plan to import users from AD and/or authenticate users against AD, the server needs to be a member of the AD domain the users are in.

Note:

If you choose to use Microsoft Active Directory, you must have the rights to:

- Assign Internal DNS Names to IP Addresses
- Create Global Security Groups and assign User/Group memberships in the AD.

Client Requirements

G/On currently has two client versions to choose from.

- G/On USB
- G/On Desktop

G/On does not technically limit which clients you choose to deploy. You should receive your G/On USB keys in the package together with your software. The desktop clients can be found in the `Emcads/GOnDesktop` folder on the G/On Server once you have completed your initial installation and configuration.

Client Firewall Requirements

G/On requires that Port 3945/tcp (or other ports as configured in G/On builder, see later) is open for Outbound traffic on all clients.

Optional http proxy tool is available for special configurations where clients need to traverse http proxies from within an internal network to get access to the Internet. More details in Chapter 13.

Client Hardware Requirements

G/On USB

USB port version 1.1 or higher

Minimum two virtual drive mappings available before any network drive mapping (e.g. drives E:\ and F:\)

G/On Desktop

Available hard disk space: 40 Mb

Client Software

Your G/On Clients can use one of the following:

G/On USB

Microsoft Windows 7 Release Candidate[3] *(32 bit and 64 bit)*

Microsoft Windows Vista and Vista SP1 *(32 bit and 64 bit)*

Microsoft Windows XP SP2 incl. Hotfix KB884020

Microsoft Windows XP SP3

Limited support for Windows 2000 Professional SP4 (*please contact Giritech support for details*)

G/On Desktop

Microsoft Windows 7 Release Candidate[3]

Microsoft Windows Vista and Vista SP1

Microsoft Windows XP SP2 incl. Hotfix KB884020

Microsoft Windows XP SP3

Limited support for Windows 2000 Professional SP4 (*please contact Giritech support for details*)

[3] Note that G/On 3.6 is released prior to the final release of Windows 7.

DNS Settings

Using External DNS Names

To enable external, remote access, you may want to define a DNS record, for example, `gon.company.com` that you can map to the firewalls external IP address assigned to the G/On Server.

We recommend that you use Host Names instead of IP addresses. This puts fewer requirements on you to reconfigure & redeploy your users/clients if you change the external IP address of the G/On Server.

When to use Split DNS

Some third party products may require Split DNS service, like Citrix PN, Microsoft Outlook, and Microsoft CRM. For more information on when and how to use split DNS, consult the Support section on the Giritech website.

Anti-Virus Settings – Server side

If you have an anti-virus application on your server, we recommend you except the temp directory from background scanning. The reason for this is that the EDMS (EMCADS Data Management System) needs exclusive access to its own temporary files, which are created in the temp directory.

In case of "false positives" where an installed AntiVirus solution falsely identifies G/On as malware, please contact Giritech Support for help to contact the vendor and resolve the issue.

Database Setup

G/On includes support for three types of databases

EDMS (Giritech's Native **E**MCADS **D**ata **M**anagement **S**ystem)

MS SQL Server 2005[EP]

MS SQL Server 2008[EP]

G/On EDMS

If you choose to use the Native EDMS, no pre-configuration is necessary.

MS SQL Server 2005 and 2008[EP]

For users of MS SQL, you need to follow a specific series of actions to prepare your MS SQL environment for G/On. For detailed information how to install with the appropriate settings, please refer to the document **SQL 2005/2008 Configuration** located on the Giritech website under *Support*.

> **Note:**
>
> You do not need to create a database. The database will be created by G/On Builder during the installation and configuration process. More Information can be found in Chapter 3.

Using Virtual Servers

G/On 3.6 supports the installation of G/On on virtual servers using the Tokenless Option option. This is a license option that needs to be ordered together with the G/On Server to enable installation without a USB server token in the server.

The rest of the installation follows the standard G/On installation guidelines as outlined in the remainder of this document.

SECTION CHECKLIST
❒ Did you Verify your server meets the Software and Hardware Requirements
❒ Did you review your Bandwidth?
❒ Is the G/On server placed in the recommended location in your environment?
❒ Have you configured your Firewall?
❒ Did you open Port 3945, 443 or 80 OUTBOUND, unrestricted on the Firewall to activate and upgrade your G/On installation or agree with Giritech Support to use the *Offline license* option?
❒ Do you have the necessary hardware, IP addresses or PAT configured for Failover?
❒ Is your User Directory configured with trust to the appropriate domains?
❒ Do your corporate PCs meet the client Software & Hardware Requirements?
❒ Have you established all the External DNS Settings?
❒ Have you prepared your MSSQL Database or will you use the Native EDMS?
❒ Have you read the stipulations for use of Virtual Servers?

Chapter 3

G/On Installation & Server Configuration

Chapter 3 is a walkthrough of an initial installation of G/On. If you are upgrading from a previous version of G/On, there is a complete walkthrough & reference guide for upgrading in Chapter 5.

Now that you have completed the necessary Environmental preparations outlined in Chapter 3, we will get started installing installing G/On. This chapter covers the initial installation of G/On of G/On Using G/On Builder.

Installing G/On

Unpacking your G/On Product

When you receive the G/On product, it consists of the following:

One black USB key. - This is referred to as the "server token" and is needed for the G/On Server installation, configuration and execution.

> ! Must always be present in the G/On Server unless the Tokenless Option feature has been enabled. Please consult your order acknowledgement to verify. The black server key is however, included with all G/On packages as a “proof of license”.

Red/white USB keys with G/On print. - These are user (client) keys.

Note:

One of the red/white user keys is specially marked, containing the file EDCSERIALS.DAT. Set this aside now, as you will need to copy this file to the G/On Server after you have completed the server installation and before you deploy user keys.

A CD-ROM containing G/On Product Software, Electronic Documentation & Desktop Client

Installing the Software and acquiring the first License

1. **Insert the server token in a vacant USB port on the server.**

When Tokenless [Option] is enabled, go directly to step 2 and have your license number available and follow the onscreen license validation steps.

Note:

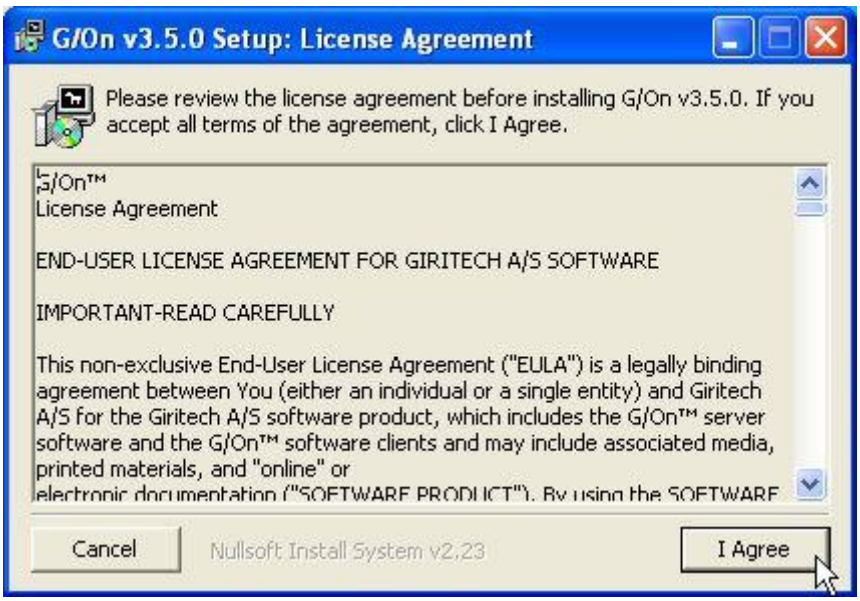
In Windows Explorer you will see how the USB key mounts two drives and assigns drive letters. If the assigned drive letters conflicts with existing drive letters (local or network mapped drives), you can assign other drive letters for the USB partitions. This is done by running `diskmgmt.msc`, right clicking on the partition in question and choosing "Change Drive Letter and Paths."

2. **Insert the G/On product CD.**

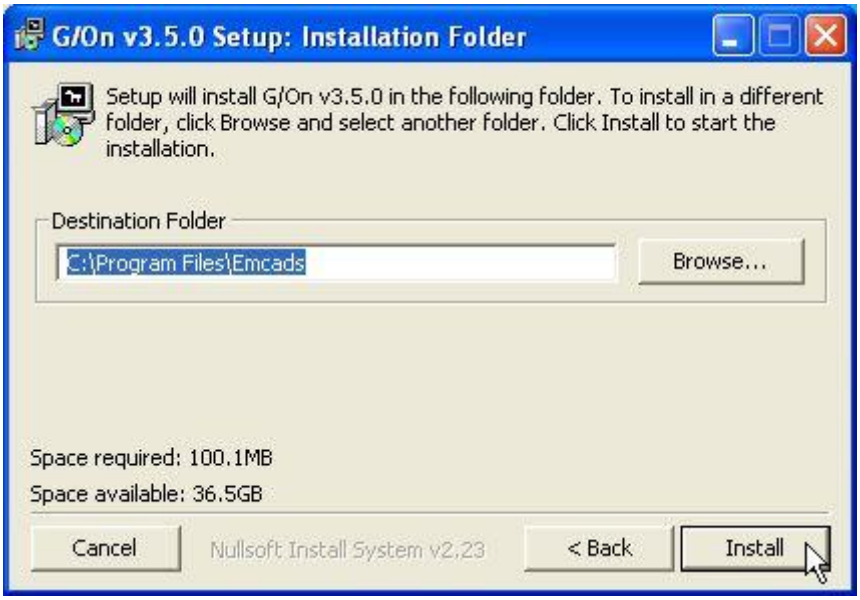
If auto-run is enabled on the Windows server, you should be prompted to run and install G/On.

If auto-run is disabled, you can start the installation by starting "InstallGOn.exe" from the root of the CD.

3. **Read the license information; accept these by clicking on "I Agree", and the server installation starts.**


G/On v3.5.0 Setup: License Agreement
Please review the license agreement before installing G/On v3.5.0. If you accept all terms of the agreement, click I Agree.
G/On™
License Agreement
END-USER LICENSE AGREEMENT FOR GIRITECH A/S SOFTWARE
IMPORTANT-READ CAREFULLY
This non-exclusive End-User License Agreement ("EULA") is a legally binding agreement between You (either an individual or a single entity) and Giritech A/S for the Giritech A/S software product, which includes the G/On™ server software and the G/On™ software clients and may include associated media, printed materials, and "online" or
Cancel
Nullsoft Install System v2.23
I Agree

4. **Choose where to install the server product.**
   Default is `C:\Program Files\Emcads\`, but you can install the product anywhere on a local hard disk.


G/On v3.5.0 Setup: Installation Folder
Setup will install G/On v3.5.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Emcads
Browse...
Space required: 100.1MB
Space available: 36.5GB
Cancel
Nullsoft Install System v2.23
< Back
Install

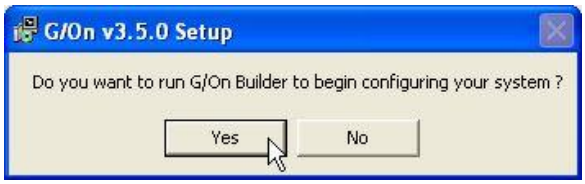
5. **Press the INSTALL G/On Server button.**

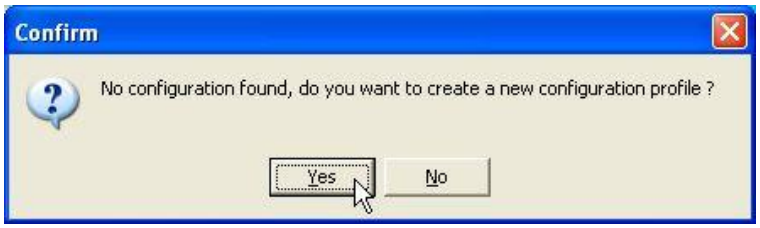
6. **Make sure the black Server Token is inserted in a USB Port (see 1.). Click OK.**

   Or, in the case of a Tokenless Option **installation, follow the onscreen licensing directions.**

G/On v3.5.0 Setup
You are now about to install G/On.
At this time you should verify that the Server Token you received
with your installation package is inserted in the USB interface on the server you are installing.
Before attempting offline license activation, please contact your Giritech partner
OK

7. **Respond Yes to the first three screens that appear:**





Initial License Activation

8. **Request a license from the Giritech license server by answering "Yes" in the window shown below. *Before confirming please make sure the G/On server has access to the Internet and is allowed to contact `license2.giritech.com on port 3945/tcp`!***

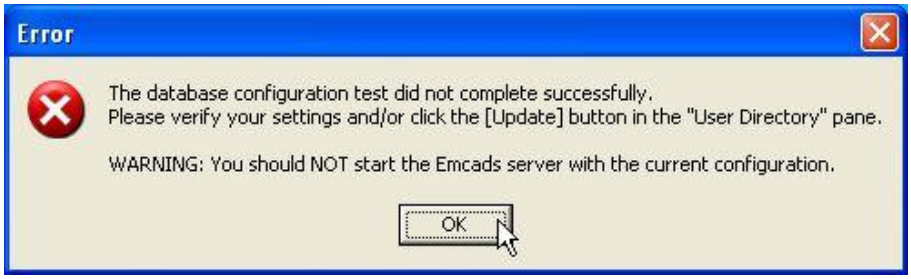
Note:

If the server cannot get access to the Giritech license server, the following error message (see screenshot) will be presented up to three times (when trying ports 3945, 443 and 80 respectively). If all three attempts fails, the license acquisition will fail and G/On Builder will be launched enabling you to perform an Offline installation. Please contact Giritech Support if this situation should occur for help with the offline installation and go directly to step 11.

9. **An activity indicator ("Working") will be shown while the G/On server tries to connect to the Giritech license server. Finally you will be requested to save the received license as shown below:**

10. **Press "Yes" and read the following message carefully (see below) and accept by pressing "OK". This message is caused by a missing G/On database and will only occur when installing a new G/On server. The**

missing database will be created later. Proceed to the next section about the Builder Tool (page 23).


Error
The database configuration test did not complete successfully.
Please verify your settings and/or click the [Update] button in the "User Directory" pane.
WARNING: You should NOT start the Emcads server with the current configuration.
OK

Offline License Activation

11. **Offline license activation involves the following steps:**
    - **Contact Giritech support!**
    - **In G/On Builder under the "File" pane select "Offline license activation"**
    - **In the popup window (see below) a "Hardware ID" will be presented. Forward this number together with your license number (from the order confirmation or on the G/On box you received) to Giritech support**
    - **Giritech will return a "License string", either via email or directly on the phone, that you need to paste into the "License String" field (see figure below).**
    - **Press OK**
    - **Verify that the license details in the main G/On Builder windows under "Server" pane corresponds to the order confirmation you received with your G/On package (Concurrent users, Max EDCs, Expiry date and Activated Features).**

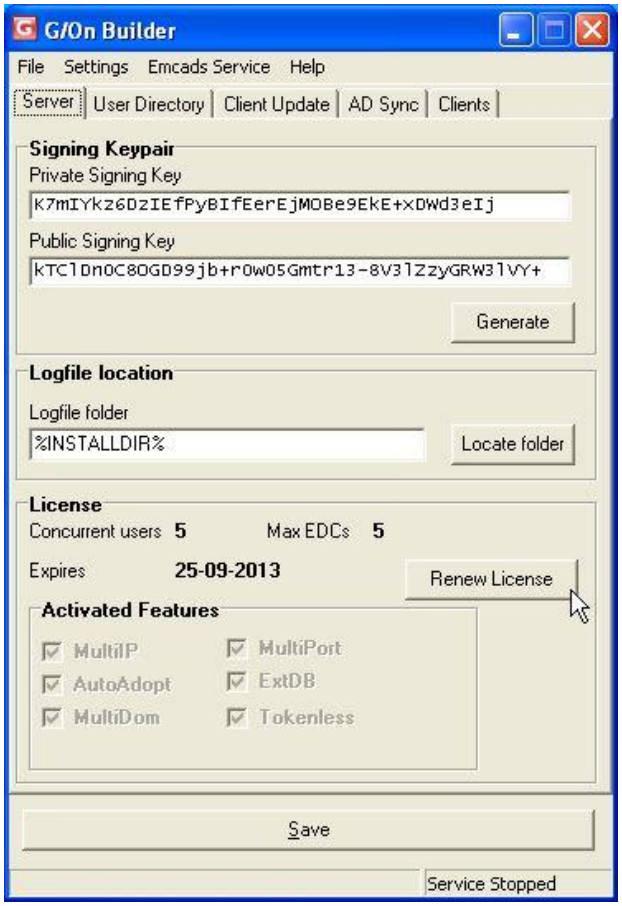
Congratulations! Your G/On Server is now installed

You may now proceed to the next section to verify your license and configure your G/On Server Settings.

G/On Builder

G/On Builder is the tool you will be using to:

- ❒ Configure your Server
- ❒ Maintain Your License
- ❒ Create Your Database
- ❒ Configure your G/On Security Settings.



The Primary Interface consists of 4 Drop-down Menus and 5 Tabs which you will use during the configuration. The next sections will walk you through the necessary settings for the:

- **Server**
- **(Advanced) Settings**
- **User Directory**
- **Client Update**
- **AD Sync**
- **Clients**

Warning:

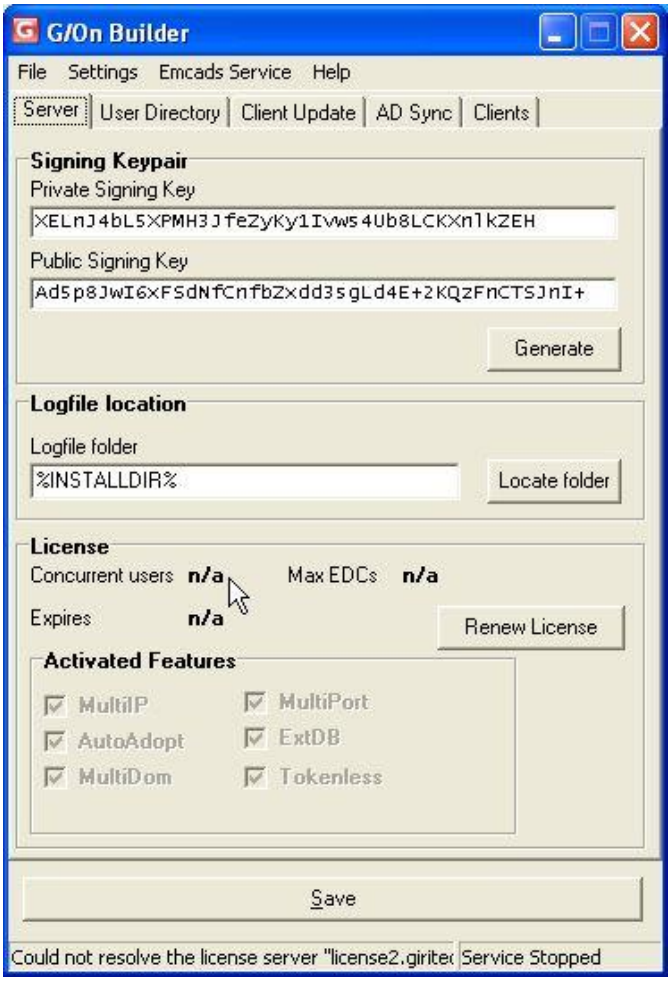
Changes to settings in G/On Builder are ONLY active after

- ❒ **You have saved and activated using the >Save Button**
- ❒ **Started/Restarted the Services using the >Emcads Service >Start or Restart**

Copyright Giritech A/S 2009

G/On Server Settings and License Activation

The **Server** tab contains three settings: Signing Keypair, Logfile location and License:



Verifying your License

1. **Start your Builder Configuration by verifying the contents of your G/On license. If no license details are presented ("N/A"), try pressing the "Renew License" button at the right hand side of the G/On builder Server Window.**

Once the license has been received[4], you will see the amount of users and tokens, the expiration date and the extended feature set of your newly received license in the "License" section of the Builder window.

The extended feature set can be any combination of below features:

MULTIIP [EP]: Support for multiple server IP addresses for server fail-over
MULTIPORT [EP]: Multi port connectivity for increased outgoing connectivity.
AUTOADOPT [EP]: Auto-adoption of clients
EXTDB [EP]: Support for external MS SQL database.
MULTIDOM [EP]: Support for multiple AD domains.
TOKENLESS [Option]: Support for installations without USB server key, e.g. virtual servers.

Signing Keypair

A **Signing Keypair**, are the private and public keys (i.e. passwords) that the G/On Server uses to identify its clients and vice-versa.

[4] Please contact Giritech Support if a license is not received! This issue is most likely be caused by the G/On Server not having access to the Internet and not being allowed to contact the Giritech license server.

Warning: Generating Signing Keypairs

Never Use the *Generate* button on a running system, unless you plan to redeploy new USB keys and Desktop Clients to all users. Generating a Signing Keypair should only be done on NEW INSTALLATIONS as all deployed keys will cease to work because they no longer "share a secret" with the server (the identity file is wrong). To redeploy, you need to distribute the new identity file. Therefore ALWAYS backup the signing keypair as one the very first actions you take when installing a G/On server.

1. ***If this is the first time you Install G/On*, Click Generate in the signing keypair section.**

2. **Copy the Signing Keypair to a file (e.g. by double-clicking and copy/paste into a text file) and store it in a secure location.**

Advanced Server Settings

Now proceed to the advanced server settings by Clicking on the Settings, Advanced Server Settings to call up the dialog box.

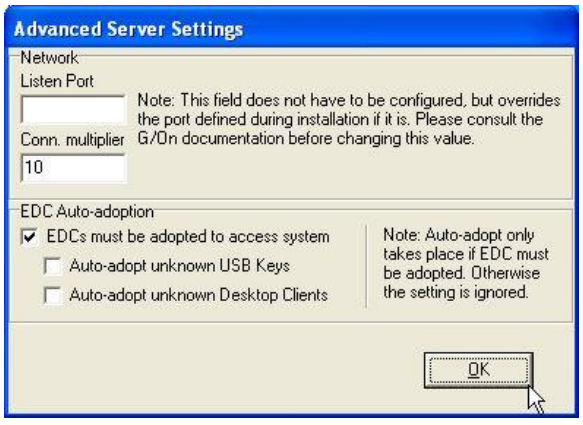
Network

This is where you set the default G/On Server Listening Port.

By default the field is empty, meaning the port is set to 3945, which is the port assigned by IANA to Giritech traffic.

For more information on the IANA port assignment go to:
http://www.iana.org/assignments/port-numbers

1. **Configure the Listen Port:** Enter the relevant port if the firewall Port Address Translates (PATs) to a different port than the port the GON server listens on, (e.g. if clients connect to port 3945 but the Firewall PAT's the external port 443 to it, enter 443). If left blank the server will simply listen on 3945.


Advanced Server Settings
Network
Listen Port
Note: This field does not have to be configured, but overrides the port defined during installation if it is. Please consult the G/On documentation before changing this value.
Conn. multiplier
10
EDC Auto-adoption
EDCs must be adopted to access system
Auto-adopt unknown USB Keys
Auto-adopt unknown Desktop Clients
Note: Auto-adopt only takes place if EDC must be adopted. Otherwise the setting is ignored.
OK

Warning:

If you change this setting on an already running system, clients will be unable to connect, unless you correctly PAT the connection on the firewall.

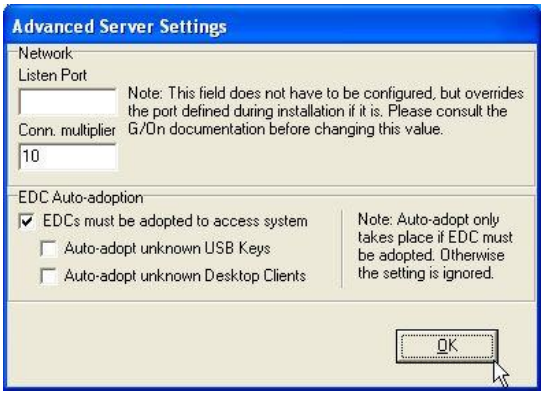
Note:

Changing the listen port number allows several separate G/On servers with different listening ports to be running on the same physical server hardware (or virtual server hardware). To use this feature, the Firewall should be configured to forward external requests from G/On clients to the relevant G/On server on the inside on the ports they have been configured to listen**.**

EDC Auto-Adoption[EP]

The last panel lets you enable or disable the level of security for EDC Access and select the auto-adopt for your clients.

- **EDCs must be adopted to access system**: This checkbox enables you to turn on or turn off the adoption validation of G/On clients (EDCs).


Advanced Server Settings
Network
Listen Port
Note: This field does not have to be configured, but overrides the port defined during installation if it is. Please consult the G/On documentation before changing this value.
Conn. multiplier
10
EDC Auto-adoption
EDCs must be adopted to access system
Auto-adopt unknown USB Keys
Auto-adopt unknown Desktop Clients
Note: Auto-adopt only takes place if EDC must be adopted. Otherwise the setting is ignored.
OK

- If you do not check the option "EDC's must be adopted" you effectively leave your G/On installation without any token security. Giritech recommends that you leave the EDC's must be adopted to access system Checked.

- Using Auto-Adoption. This option lets anyone with a USB key/Desktop Client and your identity file connect to the server. While this presents you with a way of automatically adopting keys that connect, which might come in handy if you plan a big rollout, you should also note the Warning Box below

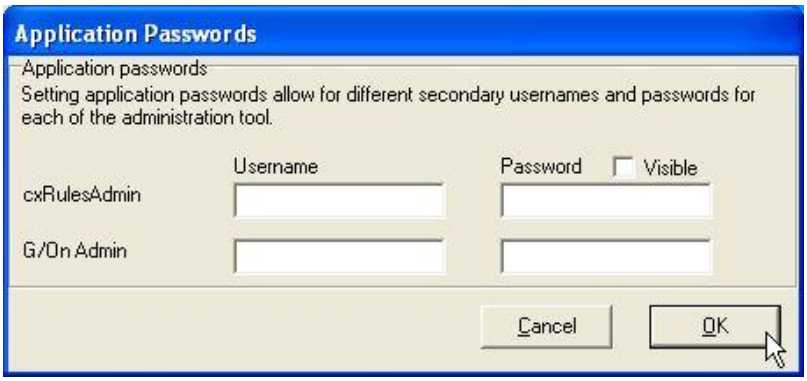
If you wish to follow security best practice Guidelines leave the default setting with the Box "EDC's must be adopted to access System" checked.

Warning:

Be aware that auto-adoption allows *anyone* with a G/On client and your identity file to connect to your server. Giritech recommends to only use this feature for a short and limited period to help large-scale rollouts of clients and not as part of normal day to day operation.

Enabling different admin application passwords

The other setting under the “Settings” menu: “Application passwords”, enables the setting of different username and passwords for the other G/On administration tools: “cxRulesAdmin” and “G/On Admin”.



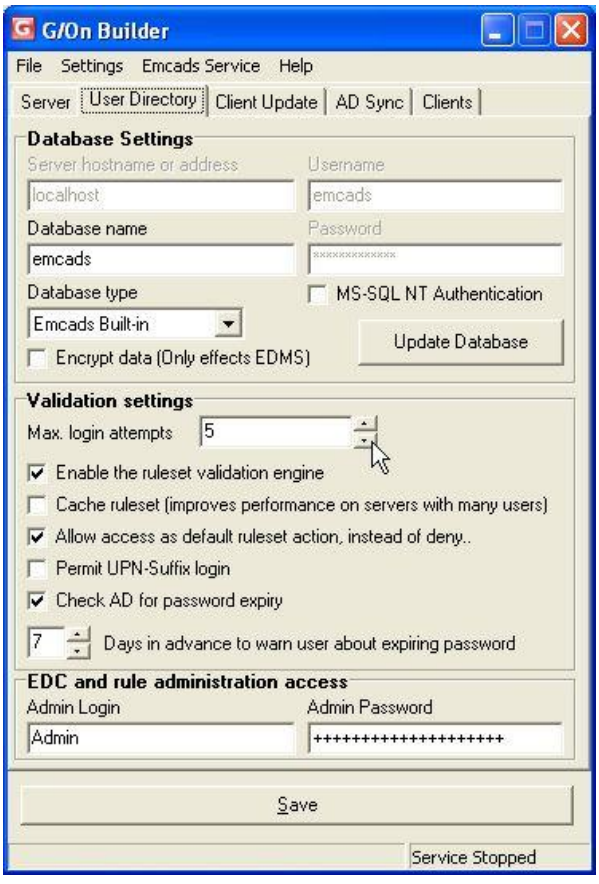
This feature has been added to support the different administration roles typically involved in Enterprise G/On installations. Managing the actual G/On installation (G/On Builder, with the Master username/password that works with all tools), managing users and their menus (In G/On Admin) and managing tokens and zones (in cxRulesAdmin) are often separated on different administrative users. The “Application Password” settings enable the G/On manager to enable roles based access to different parts of the G/On system.

User Directory and Database Configuration

The **User Directory** tab is where you define the:

- ❑ Database Settings
- ❑ User Validation Settings
- ❑ Administrator Password

1. Start by selecting the type of Database you will be using for your G/On installation.
2. Follow the instructions below for your Database setup.



Database Settings

As default the G/On Server uses an embedded **Emcads Built-in** database (EDMS).

EMCADS Built-In

If you use EDMS, the server is always “localhost”. The name of the database is `emcads` by Default. Simply click **Update Database** to enable this option and respond “yes” to the 2 dialog boxes.

Microsoft SQL Database[EP]

1. **Enter the name of your MSSQL database in the following format: “servername”\”name of MSSQL Database”.** For more information, consult Chapter 2: Configuration of Database section. You should use the same settings here as you defined when installing the MS SQL database.
2. **Update the Username and Password Fields.** Use the same Username and Password that you defined when installing your MSSQL database.
3. **Press Update Database.**

> **Note:**
>
> MS SQL NT Authentication uses the credentials of the EMCADS process to validate against the MS SQL server and NOT the Username and Password in the Database Settings Fields.

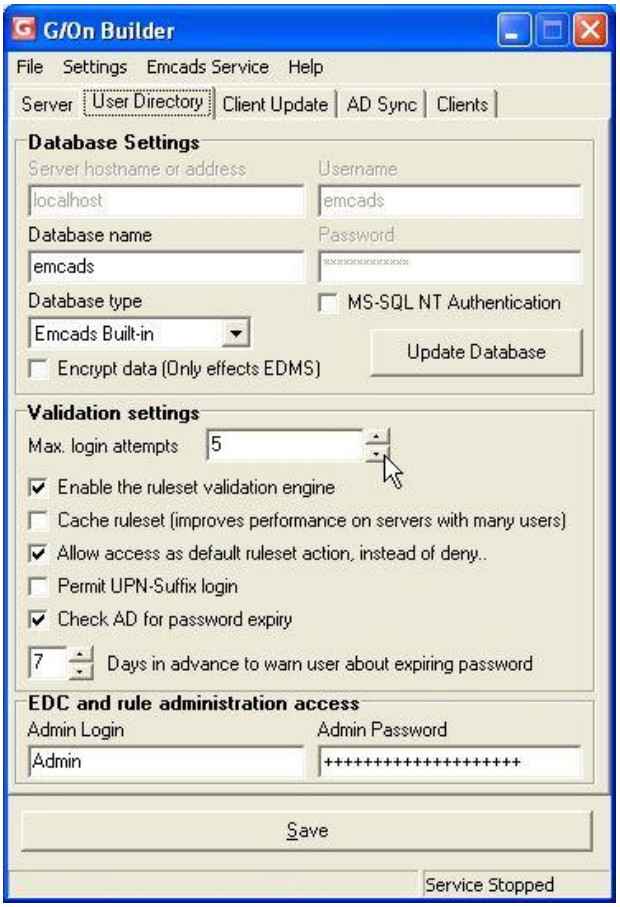
MySQL Database[EP]

The last option is to choose MySQL. This is done by selecting "MySQL" in the Database. Note that we only recommend using MySQL if it is already installed and requested by the customer. Support is limited to MySQL version 4.0.21; attempting to use other versions may cause errors. If you do not already have a copy of this version of MySQL contact: support@giritech.com.

1. **If you use MySQL, enter the IP address of the MySQL server.**
2. **Username and Password as defined by your MySQL Server**
3. **Update Database.**

Validation Settings

The Validation settings determine the general rules for how your G/On installation will validate various aspects of your Installation. Many of these settings are options but we have provided guidelines for best-practice and recommendations in the sections below. You should review each setting carefully.



Max. login attempts:

This setting determines the number of failed login attempts before the user account is locked. Once a user has been Locked Out, only the G/On Administrator can unlock and re-activate the user's account. For more information on re-activating users, consult the section for the USER tab in the G/On Admin chapter.

- **Select the number of failed login attempts you will allow before locking a user.**

Enable the rule set validation engine:

Other than allowing/disallowing clients based on whether the EDC is adopted or not, G/On lets you set up validation rules. These connection rules are based on access zones which are defined in the AccessRules Manager.

Note:

If you turn this function off, zone validation is also turned off. And you will be unable to define zones or access rules for your G/On installation.

- **Check the box to "Enable the Ruleset Validation Engine"**

Cache Ruleset:

Checking this option will improve performance on servers with many users and rules.
Check this option if your installation contains multiple rules.

Allow access as default ruleset action, instead of deny:

This option is enabled by default. If default action is left as "deny", you will have to make a rule for each and every EDC that should be allowed to connect.

Check the option to allow access. Unless you wish to create individual rules in the Access Rules Manager for each EDC you deploy.

Permit UPN-Suffix login:

This option allows UPN suffix in logins and should be selected only by companies that use the @ in the log-in name.

If your users use the "@" symbol in their username, you should select this option. Otherwise leave this blank.

Check AD for password expiration:

This option will verify with your Microsoft AD to determine whether or not a user's AD password has expired.

If you check this option, you should adjust days value option if you would like your users to receive a warning. To do this set a value in the final box to configure the number of days before the actual expiration date the user should receive the warning.

EDC and Rule Administration Access

The section at the bottom panel contains the ***Master*** Administrator Username and Password for your G/On Solution. It is used for restricting access to all G/On Server Tools:

G/OnBuilder,

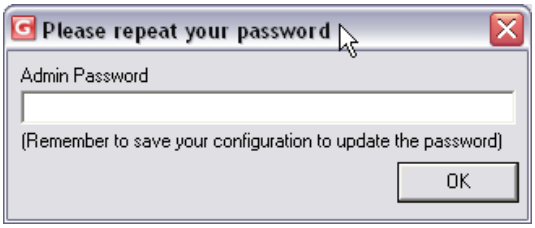
G/OnAdmin Advanced Administrator Features

CXRulesAdmin

Refer to previous section on "Enabling different admin application passwords" (page 27) to set separate passwords for CxRulesAdmin and G/On Admin. Note however that this password is the main password that overrules the other!

To Change the Default Master Password

1. **Type in your new Administrator Username and Password and select another tab (any tab will do)**
2. **Confirm the Password in the Dialogue box that appears.**



Note:

The G/On administrator password can be any string of characters, and is case sensitive. Minimum length is 5 characters, if you do not explicitly set a password, the default password is "Password" (no quotation marks, capital P)

Warning:

If you lose your Administrator Password, you will no longer be able to use any of the G/On Tools or upgrade your installation.

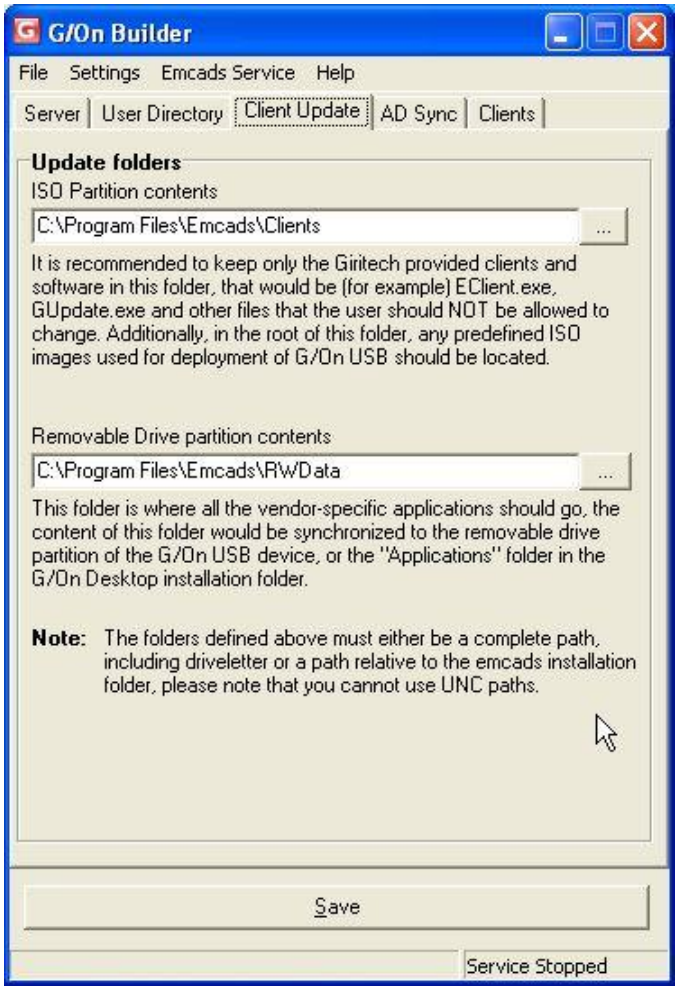
Client Update Folder Settings

This panel defines where the G/On Server stores the Client Software.

We have entered the default folders that we recommend using. If you wish to use the default settings (recommended), you can proceed to the next Tab "AD Sync".

Should you choose to change the default settings you should familiarize yourself with the Read/Only Partition and the Read/Write drive Partition described below.

There are two folders – Read/Only Partition at the top, and the Read/Write drive partition at the bottom. We recommend using the Read/Only partition for the Giritech clients (e.g. EClient.exe and GUpdate.exe) as these are files you typically do not want users to modify.


G/On Builder
File Settings Emcads Service Help
Server User Directory Client Update AD Sync Clients
Update folders
ISO Partition contents
C:\Program Files\Emcads\Clients
It is recommended to keep only the Giritech provided clients and software in this folder, that would be (for example) EClient.exe, GUpdate.exe and other files that the user should NOT be allowed to change. Additionally, in the root of this folder, any predefined ISO images used for deployment of G/On USB should be located.
Removable Drive partition contents
C:\Program Files\Emcads\RWData
This folder is where all the vendor-specific applications should go, the content of this folder would be synchronized to the removable drive partition of the G/On USB device, or the "Applications" folder in the G/On Desktop installation folder.
Note: The folders defined above must either be a complete path, including driveletter or a path relative to the emcads installation folder, please note that you cannot use UNC paths.
Save
Service Stopped

The Read/Write drive partition is typically used for 3rd party application software such as a Citrix ICA or Microsoft RDP client.

You can however freely decide which directories to use for what files.

***Note*: Many 3rd party clients need to write to configuration files during operation. If these clients are placed in the "Read/Only partition" they will not work correctly.**

When using more than one G/On Server, either because of the amount of users or because of redundancy, it is possible to place the G/On Client software for the G/On USB Key and G/On Desktop Client on a file share. This ensures all G/On Servers will distribute the same G/On Client software to all G/On Clients.

When using file shares for the G/On Client software, G/On Builder should be configured with the full UNC and not drive letters. E.g.:

\\FILESERVER\GOn\Clients and

\\FILESERVER\GOn\RWData

Note:

In G/On Builder there is a note *not* to use UNC, you can safely ignore this note.

Note:

The EMCADS service should also be changed from running under the Local System account, to run either as a service account or a user account which has read rights to the configured UNCs.

For the Desktop Client

These files are also deployed to the desktop client, however here the default path is:

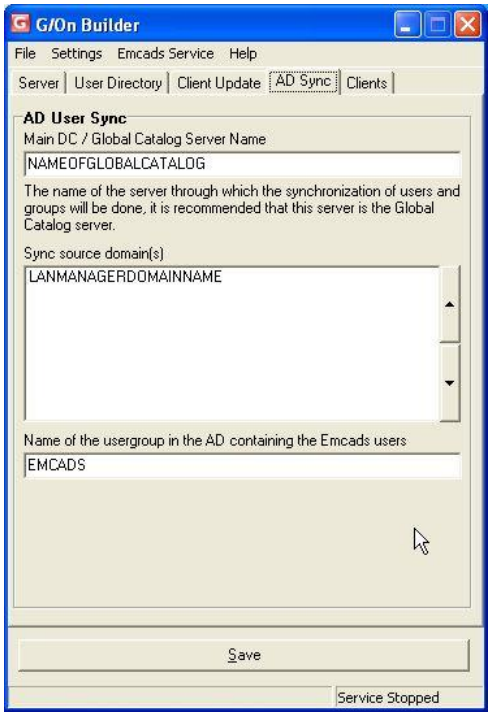
C:\Program Files\GOn Desktop.

If the user wishes, they can choose another directory when deploying the standard G/On Desktop Installer.

AD Sync

This tab is where you define the standard settings to synchronize your Active Directory and your Synchronization Domain.

These settings are valid for both versions of the Active Directory synchronization tools, USync and AdSync. However only the default USync tool can be launched from within G/On Admin (File->Sync AD). Refer to page 60 for more details.


G/On Builder
File Settings Emcads Service Help
Server User Directory Client Update AD Sync Clients
AD User Sync
Main DC / Global Catalog Server Name
NAMEOFGLOBALCATALOG
The name of the server through which the synchronization of users and groups will be done, it is recommended that this server is the Global Catalog server.
Sync source domain(s)
LANMANAGERDOMAINNAME
Name of the usergroup in the AD containing the Emcads users
EMCADS
Save
Service Stopped

Note:

If you are not using the AD for User Synchronization & Authentication, you **MUST** remove the Sync Source Domain from this Tab (right click on "LANMANAGERDOMAINNAME" and select "remove").

There are three fields in this Tab that needs to be filled in:

Main DC/Global Catalog Server

1. **Enter the name of your Main DC or Global Catalog Server in the field provided.**

This is the NetBIOS name, not the DNS name

LOCATING YOUR DOMAIN NAME

It is very important that you enter the correct information for the Global Catalog and the Domain names.

If you do not know your Domain name, you can open a command prompt and type:

nbtstat -n;

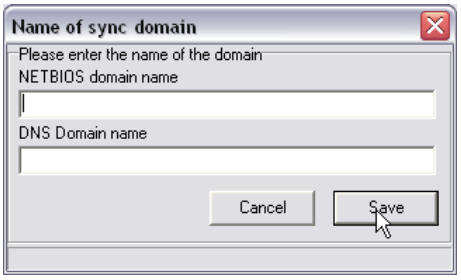
The Domain name is readable in the first paragraph of the output, in the line with (1E). This value holds the domain the server is a member of.

Sync Source Domain(s[EP])

This field holds the LAN Manager Domain names that are used for AD synchronization.

The name of the domain from where the users are synchronized and validated, this should be the “Pre -Windows 2000 Domain Name” or “LANManager domain name”.

2. **Highlight and right-click on the example “LANMANAGERDOMAINNAME” and delete it from the list**
3. **Right-click anywhere in the field and chose "Add" to add a domain name to the list.**
4. **In the window that appears, enter the NETBIOS domain and tab. If the DNS Domain Name does not Auto-resolve, manually type in the DNS domain name in the window and click Save.**

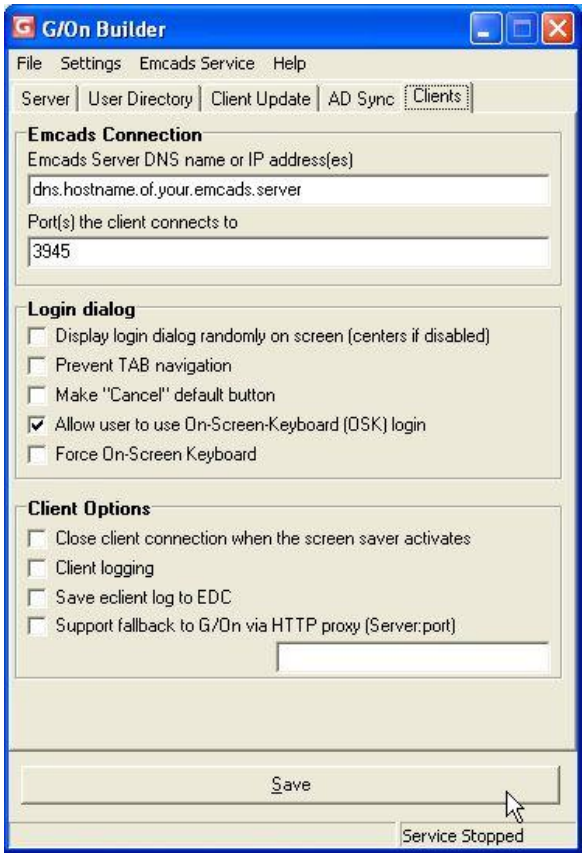


AD User Group

5. **Enter the name of the AD User Group.**

Use the name of the User Group that contains your G/On users. If this group is not created in the AD, please specify a global security group that will be using the EMCADS server.

Clients


G/On Builder
File Settings Emcads Service Help
Server User Directory Client Update AD Sync Clients
Emcads Connection
Emcads Server DNS name or IP address(es)
dns.hostname.of.your.emcads.server
Port(s) the client connects to
3945
Login dialog
Display login dialog randomly on screen (centers if disabled)
Prevent TAB navigation
Make "Cancel" default button
Allow user to use On-Screen-Keyboard (OSK) login
Force On-Screen Keyboard
Client Options
Close client connection when the screen saver activates
Client logging
Save eclient log to EDC
Support fallback to G/On via HTTP proxy (Server:port)
Save
Service Stopped

The Clients Tab contains all the settings that will define the address where clients connect, and the behavior of the client to the end-user.

EMCADS Connection

Here you enter the DNS name or IP address(es) of the G/On Server, as well as the specific port(s) that the client should connect to. We recommend 3945, the port assigned by IANA to Giritech traffic.

Reference:
http://www.iana.org/assignments/port-numbers

Multiple addresses and ports configuration:

The G/On client can be configured to connect to alternative addresses and/or ports, increasing connectivity from clients that:

- suffer from restricted outgoing ports (the MULTIPORT[EP] feature must be enabled, see page 24),
- have set-up more G/On servers for failover (the MULTIIP[EP] , Tokenless[Option], and EXTDB[EP] features must be enabled and failover configuration established, see page 24)

You can specify up to 5 IP/DNS addresses and/or 5 ports.

The Addresses and ports are paired comma-separated. The connection will occur on the first combination of server address and port, where a G/On server answers the connection attempt.

Example:

Server: DNSname1,DNSname1,DNSname1,DNSname2

Port: 3945,5000,443,3945

In this case, the client first tries to connect to DNSname1; first on port 3945, then 5000, then 443, and finally the client will attempt to connect to DNSname2 on port 3945.

The number of server addresses must at least be the same as ports to connect to. If the number of ports exceeds the number of addresses, probing for servers stops when the last address has been tried and thus ignores the remaining ports.

Copyright Giritech A/S 2009

Note:

The server still only listens on the designated listen port. You will have to configure multiple PATs on the firewall, or by other means forward the server's listening port to listening ports on the configured addresses, or alternatively install more G/On servers[EP].

Login dialog

These are the settings for the behavior of the client login interface. The first three boxes are settings to make it more difficult to script a G/On login, increasing client login security.

Display Login Dialog Randomly

Prevent Tab Navigation in the Login Dialog

Make “Cancel” the default button instead of “Enter”.

The next two boxes allow you to offer or even force the use of the OSK (On-Screen-Keyboard), which is an effective way to cheat keylogger software.

- **Select which of the 5 Log-In Dialog Features you wish the clients to exhibit.**

Client Options

The bottom check boxes controls client logging and provides an option to disconnect the client from the server, if the screensaver on the client PC activates. This will reduce the risk of abuse if the user forgets his key in a logged-in machine.

- **Choose if you want the clients to disconnect when the Screensaver activates.**

Warning:

All settings on the Clients tab are stored in the identity file on the client. Changes to this tab will therefore not occur until the client has been updated with the newly updated identity file. This is usually done with GUpdate.

- **If you need connection logging enabled on the clients, check the “Client logging” box. This will not *save* the log but only enable logging!**

Please note that if “Client logging” is *disabled* (default setting) there will be no “show log” entry on the menu’s of all clients.

- **Decide if you want the log to be stored (on the EDC) by checking the "Save eclient log to EDC" box.**

Security Warning:

Information in the Client Log is stored in *clear text* and may reveal sensitive information about your company infrastructure.

HTTP Proxy Support

The last box in the Client Options field is "**Support fallback to G/On via HTTP proxy**" with a field for entering a server name/IP and port address. This box support the Giritech HTTP proxy support tool delivered with G/On 3.4, 3.5 and 3.6.

Giritech "TCP over HTTP" (ToH) is a support tool to G/On 3.4, 3.5 and 3.6 that address the problem of a G/On client being a guest on a foreign network where connections directly to the G/On server is blocked, and the only access to the internet is through a HTTP proxy. I.e. when users are trying to connect from within a proxy "protected" network that is not under the G/On Administrators control.

In this scenario, a G/On Administrator can enable ToH for *his* clients and on *his* server, and thus enable his clients to connect through foreign HTTP proxies, through the untrusted internet and through his ToH server to his G/On server.

Warning:

TCP over HTTP is a highly advanced networking option requiring a deep understanding of IP networking and proxies. It is therefore strongly recommended to read appendix XX carefully to ensure a proper understanding of Giritechs implementation or to contact Giritech support for help *before* enabling this option.

Warning:

The HTTP Proxy option should never be the *only* option for G/On clients to connect to a G/On server. Only using the HTTP Proxy option will impair users ability to remotely update their clients because G/Update does not run through the HTTP Proxy tool.

Please ensure that at least one direct connection (via standard ports as described previously) to the Emcads server exists.

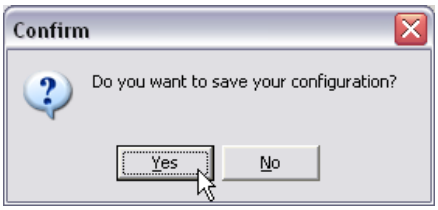
Overview of the steps required to enable HTTP proxy support please consult the Appendix on page 122 for details:

- **Read the Appendix on page 122 carefully.**
- **Check "Support fallback to G/On via HTTP proxy" if you need the G/On clients to support G/On via HTTP proxy by tunneling G/On TCP traffic as HTTP traffic through HTTP proxies. This setting tells the G/On client to communicate via the HTTP proxy server on the foreign network instead of directly to Emcads in case connections cannot be made on the standard addresses and ports.**
- **The "*server:port*" field refers to the address of *your* ToH server and is the target IP address the client side HTTP Proxy should connect to.**

Copyright Giritech A/S 2009

- **No other client settings should be required. Default settings of ToH should work under most circumstances because the client side settings of the foreign HTTP proxy will be read from local Windows settings.**

Completing and Activating the G/On Server

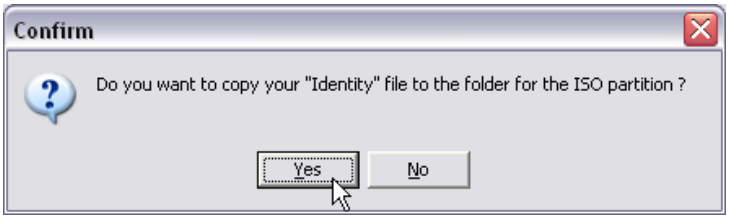


1. **Once you have filled in the five tabs of the G/On Server Configuration tool, press the "Save" button at the bottom of the Builder window.**

2. **Respond to the Dialogue Boxes**

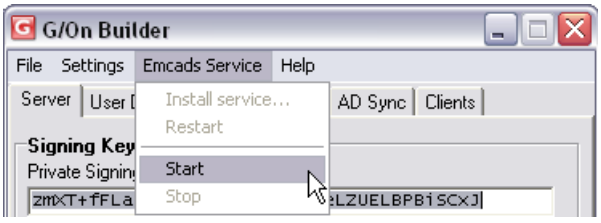
Warning:

Every time you save your configuration, you will be met by a confirmation box like the one below. If you choose "Yes", the identity file will be copied to the Clients directory as well as to the GOnDesktop directory and hence *overwrite* the existing Identity file at those locations!



The configuration settings you have made are now in force. The last thing you need to do is start the server.

3. **Go to EMCADS Service and Select START**



The server is installed as a Windows Service. You can start, stop and restart the G/On server from the Windows Services Manager (invoke services.msc), After saving and activating your configuration, service control is also possible from the menu item "Emcads Service" as shown on the figure above. Service status is always visible in the bottom right corner of the G/On Builder window. It should now state "Service Running".

Moving G/On to another server.

Should you encounter the need for moving the software to another server, besides the Windows Registry keys added to add the windows service, files are merely copied to the new server. It is recommended to use the same locations as on the old server.

> **Note:**
>
> This scenario applies to moving an **existing** server to another box. If you wish to set up a failover server, please read the instructions on Failover Configuration & Setup

Steps to move the server (Token based):

1. Deactivate the License in G/On Builder. Start G/On Builder and use pull down menu File > Deactivate License. G/On Builder will connect to Giritech's License Manager and release this particular server license and make room for a new license on another physical server PC.
2. Take a full backup of the server including the Signing Keypair.
3. Stop the service, if running
4. Uninstall the service; this is done by invoking "emcads.exe -r -p 3945" in a command prompt. Substitute 3945 with the port number, your G/On server is configured to listen on, if applicable.
5. Copy the server root directory (default C:\Program Files\Emcads) with all files and subdirectories to the new server.
6. Move the server token to a USB port in the new server
7. Activate the license in G/On Builder using Renew License
8. Install the Windows service on the new server by invoking "emcads.exe -i -p 3945" in a command prompt. Remember to replace the default "3945" setting with the port you have decided your G/On server should be listening on.
9. If applicable, change your IP settings on the new server, so the IP address matches the one of the old server, or change firewall NAT/PAT settings and maybe also DNS settings to reflect the new IP address.
10. Start the server

Steps to move the server (Tokenless[Option]):

1. Take a full backup of the server including the Signing Keypair.
2. If you are using G/On without the G/On USB Server Token and your license permits you to only run one server (or if you have already used all the servers as permitted by your license), you need to *Deactivate* the license for the server that is no longer going to be used. Start G/On Builder and use pull down menu File > Deactivate License. G/On Builder will connect to Giritech's License Manager and release this particular server license and make room for a new license on another physical server PC.

> **Note:**
>
> If you for some reason are unable to deactivate the license, please contact your Giritech Partner who will make arrangement to have it deactivated or to increase the number of servers permitted by your license.

3. Document the G/On Builder License Configuration on the old server and take a copy of the Public and Private Key Pair and store them in a safe location using Notepad or similar text tool.
4. Copy the server root directory (default C:\Program Files\Emcads) with all files and subdirectories to the new server.
5. Start G/On Builder and use G/On Builder to reconfigure the G/On License to the same License Configuration as on the previous server PC. Reuse the same Public and Private Key Pair from the old server.
6. Once you have configured G/On Builder do a *Renew License*. You will have to enter your G/On USB Server Token Number (your License Number) that is printed on your G/On Package and on the G/On shipping documents.
7. *Save* the configuration and *start* the G/On Service via the Emcads Service pull down menu in G/On Builder.

Installing multiple G/On servers.

Running multiple G/On servers *concurrently* (using the same license) to support failover, standby or different backup policies, the following process must be followed carefully.

To enable the multiple concurrent servers, you need to have the following ready ***before you begin*:**

1. Your G/On License must be configured for Tokenless[Option]. As this is optional, make sure the Tokenless feature was acquired for your license.

2. Your G/On License must be configured for at least the number of servers you intend to run. As a G/On License comes default with one server, make sure the needed number of servers was acquired for your license.

3. If you intend to simply make copies of your primary installation, make sure this installation is completely configured according to this G/On Admin Guide and running as expected.

4. Document the G/On License Configuration of the primary installation by either taking screen shots of each of the G/On Builder pages or write down the settings. **Copy the primary and public key pair** with a tool like NotePad and save the text file on a share where it can be reached from the other server PCs to run the G/On servers.

Now you're ready to install and run the second server:

1. Copy the server root directory (default C:\Program Files\Emcads) on the primary server PC with all files and subdirectories to the second server.

2. On the second server, delete the file **license** in the server root directory

3. Start G/On Builder and redo the G/On License Configuration. Paste in the private and public key pair from the NotePad and make sure the rest of G/On Builder is configured exactly as on the primary server

4. Do a Renew License followed by a Save & Activate.

5. Install the G/On Service via the Emcads Service pull down menu in G/On Builder. Start the service.

If you need to run more than 2 servers, please repeat these 5 steps for each additional server you need to install.

Chapter 4

Upgrading G/On

Upgrading your G/On installation is a simple procedure and as long as you haven't made any changes to the server environment, placement or structure, can be done with minimal interruption to your users.

Before upgrading your G/On Installation, there are several critical factors that you should pay attention to the in the sections on Backup and Signing Keypair in the *Prior to Upgrade* section of this Chapter. Changing these items could result in failure for all existing users and result in you having to re-deploy all your clients.

Prior to Upgrade

You should follow these steps carefully. Doing so will ensure that you are able to restore your system to it's original state or restore settings that may have been inadvertently changed during upgrade.

Warning:

G/On release 3.6 uses a new EDC detection routine for identifying the computers from which access is given. This means that *all* desktop clients adopted with G/On version 3.5 or older will have to be re-adopted after installation of G/On 3.6. **See section:** Notes on G/On Desktop Adoption **on page 106**

Backup your G/On Server

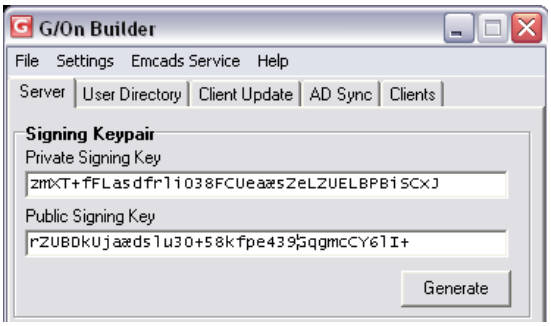
Prior to commencing the upgrade, remember to backup the G/On Server. This can be done either by actually backing up to some other media, or by simply copying the contents of the directory the G/On Server is installed in, normally *C:\Program Files\Emcads*, over to another directory.

As of version 3.2, you can also choose to use the backup and restore feature in G/ON Admin to backup the components of your installation as separate files. For more information on using this feature consult the Backup-Restore section on page 118.

Copyright Giritech A/S 2009

Copy your Signing Keypair

We strongly recommend that you Copy the "Private Signing Key" and "Public Signing Key" which you will find on the G/On Builder "Server" tab to a text file and save it to the backup location. (This will help avoid having to manually update all clients if a failure occurs.)



Notify Users

Notify your G/On users that their G/On connection may experience disconnection/interruptions during the upgrade process.

See also the Warning note on page 41.

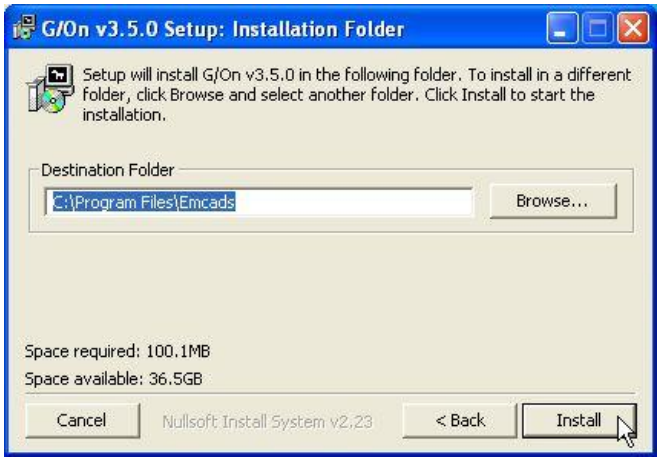
Warning:

Changes to settings in G/On Builder are ONLY active after

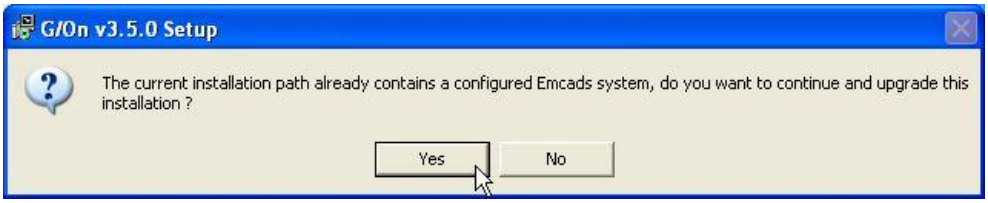
- ❒ **You have saved using the *Save* Button**
- ❒ **Started/Restarted the Services using the >EmcadsServices >Start or Restart**

Installing the Upgrade

1. **Download the G/On Installer. After closing all active G/On windows, select the InstallGOn.exe and RUN the G/On Installer**
2. **Accept the license Agreement and Select Install.**
3. **Verify that your Server Token is in place and respond OK or follow onscreen directions when running Tokenless**[Option]**. *Please remember to stop the HTTP Proxy Bypass tool as well (refer to* Introduction to the HTTP proxy tool *on page 122 for details) or you will get a write error message. Also remember to restart the HTTP Proxy Bypass server after upgrading G/On.***


G/On v3.5.0 Setup: Installation Folder
Setup will install G/On v3.5.0 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Emcads
Browse...
Space required: 100.1MB
Space available: 36.5GB
Cancel
Nullsoft Install System v2.23
< Back
Install

4. **Select Yes to Install the new version on top of the old.**
   The G/On Installer automatically recognizes an already installed version and will install on top of it.


G/On v3.5.0 Setup
The current installation path already contains a configured Emcads system, do you want to continue and upgrade this installation ?
Yes
No

5. **Once the new version is installed, select OK**
   After the upgrade is complete you will be asked to verify your installation, re-acquire your license and upgrade the database. Select “OK”.

G/On v3.5.0 Setup
You performed an upgrade of your Emcads system, therefore you MUST proceed to run G/On Builder to verify your installation and possibly renew your license..
OK

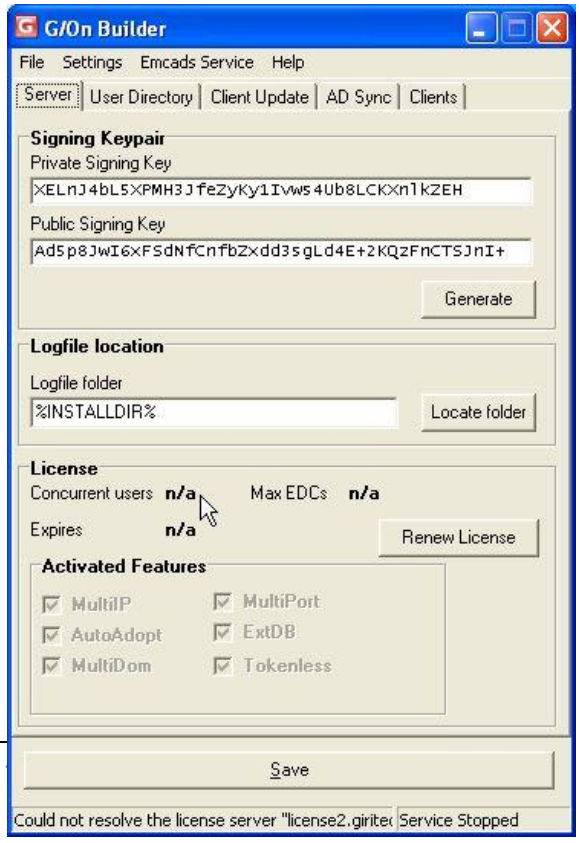
6. **Log Into G/On Builder**
   Use your existing administrator username and password to launch G/On Builder, where you will have to renew your license and Update your database.

   On the “File” menu in G/On Builder select the option to “Renew License” (Note: outgoing port 3945, 443 or 80 must be open for acquiring the license or you must go through the process for “Offline license activation”)

G/On Builder Changes during Upgrade

Changes to G/On Builder can seriously affect your entire installation. We recommend that you follow the guidelines carefully.

1. **Backup and Copy**
   If you skipped the section on Getting Started at the beginning of this chapter, we recommend that you copy your Signing Keypair at this time.
2. **Go to the Server Tab.**
3. **Renew Your License**
4. **Next go to the "User Directory" tab and press the “Update Database” button to update your existing database. DO NOT CHANGE YOUR DATABASE TYPE AT THIS TIME.**

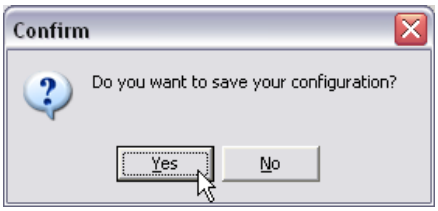


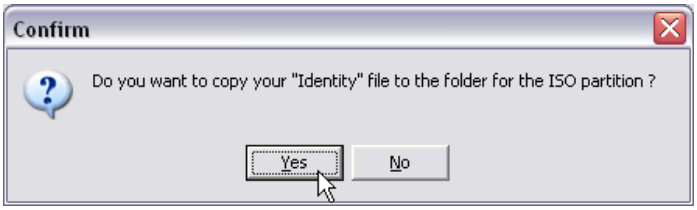
If you wish to change the type of database you are using, please consult the section on Migrating to an External Database like MS SQL

Copyright Giritech A/S 2009

(requires the feature EXTDB[EP]) at the end of this chapter.

5. **Select "OK" in the pop-up windows to confirm the test of the database connection completed successfully.**
6. **Once you have filled in the five tabs of the G/On Server Configuration tool, select the "Save" button in the bottom of the window.**
7. **Respond Yes to the Dialogue Boxes:**





Warning:

Every time you save your configuration, you will be met by a confirmation window like the one above. If you choose "Yes", the identity file will be copied to the /Clients directory as well as to the G/On Desktop directory and *overwrite* the existing Identity file.

The configuration settings you have made are now in force. The last thing you need to do is start the server.

8. **Go to EMCADS Service and Select START**
   Check the bottom of the G/On Builder window for the "Service Running" message

Upgrading your Clients to the Latest Version

After upgrading your G/On server, you will need to update your users clients. This process is controlled by the G/Update tool. You have two primary choices when upgrading your clients.

1. Send an email and request that they run G/Update from their client. For more information on manually updating clients see page 112.

2. Automating Your Client Update with Zone Rules. For more information on automating your client update see page 107

Please refer to the Warning note on page 41.

Migrating to an External Database[EP] like MS SQL Database

When migrating from the built-in EDMS to the MS SQL database, we recommend that you follow the following steps in order.

1. **Follow the upgrade instructions to upgrade your system normally. Once you have upgraded to G/On 3.6 you can migrate to the new database version.**
    a. **Backup Your G/On Installation**
    b. **Install and Upgrade from the prior version of G/On to G/On 3.6**
    c. **Update your existing Database**
    d. **Verify that you have prepared the MS SQL environment according to the guidelines provided in Chapter 2 of this Manual.**

2. **Once you have upgraded to G/On 3.6 take a full Database backup from the GOn Admin> File> Backup and Restore dialogue.**

Don't overwrite your old backup.

3. **Go to the "User Directory" Tab in G/On builder.**

4. **Change the Database type to MS-SQL and change the settings for Server Hostname, Username and Password. (More information on Settings can be found in the Chapters on Configuration Requirements and in the Installation and configuration Section of this manual.)**

5. **Update the Database**

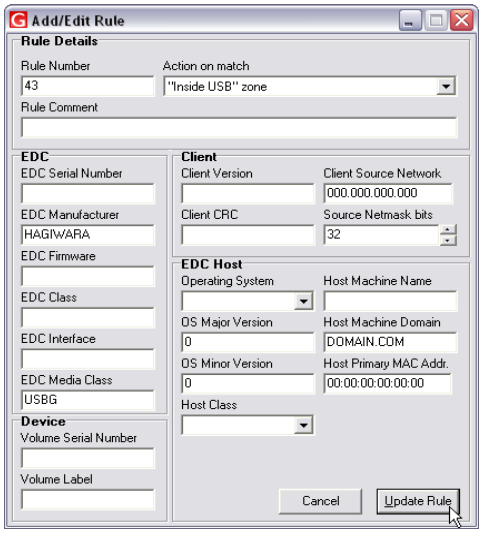
6. **Restore your database, that you created in step 2 above, from the GOnAdmin>File>Backup and Restore Database function, into the New MS SQL database.**

Changes to Zone Rules for USB Keys (pre-3.3)

The following is only relevant when upgrading from a pre-3.3 G/On installation.

As of Version 3.3, and onwards, you need to review all Zone Rules that Apply to USB Keys. Version 3.3 (and onwards) includes new features for G/On Client Carrier, the EDC. The new EDC recognition will require you to take action to create a new zone Rule.

Background: We have prepared G/On for a new G/On USB architecture that will allow us to support much larger USB keys. As part of this process, G/On 3.3 (and onwards) is detecting an increased level of detail from the G/On Keys.



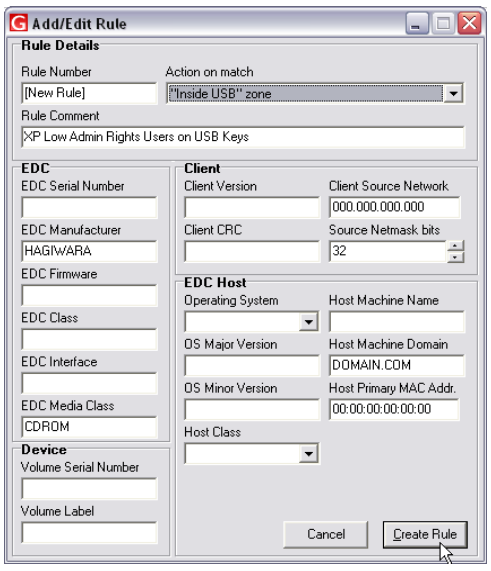
Benefit: The new USB detection routine is now reporting more details on the EDC Media Class Field and hence helps increase the overall security of the solution.

Upgrading from pre-3.3.1: existing zone rules will be converted to comply with the new USB reporting as follows:

- ❒ If the EDC Manufacturer is HAGIWARA then EDC Media Class – will be changed to – USBG

In this example (see figure from AccessRulesManager), we have an Inside Rule for USB Keys. It states that Our Hagiwara Keys registering USBG logging in from our domain PCs - DOMAIN.COM (for example GIRITECH.COM) will be assigned to the Inside Zone.

This new detection is available for USB Keys when logging in from Windows XP as an Administrative User or from Windows Vista – as a Standard or Administrative User



Note: Special settings are required for users on Windows XP – logging on as a Non-Administrative or Low User Privileges.

The new detailed detection levels are only available for XP Administrative and Vista Standard/Administrative Users. In order to enable your users to access G/On from XP clients where they do not have administrative Rights**, you will have to create a second zone rule** that includes CDROM in the EDC Media Class.

In this example (see figure), we have created a second Inside Rule for USB Keys. It states that Our Hagiwara Keys registering CDROM logging in from our domain PCs - DOMAIN.COM (for example GIRITECH.COM) will be assigned to the Inside Zone.

This action should be repeated for all zone rules that you would like to make available to users on XP without Administrative rights.

Copyright Giritech A/S 2009

Chapter

5

Zone Configuration with the G/On AccessRules Manager

G/On allows you to control what level of client access should be allowed based on your level of Trust for the client and it's location. "Zone Rules" reflect this level of trust versus access each user receives.

In this section you will learn how to define zones and create rules for what users can access based on your level of trust for the user, his location and the computer being used.

When a client connects to a G/On server, information about the PC's hardware, software and the connection itself is collected and sent to the server. Matches on certain details of this information can be used to flag the connection with a name. This name is a Zone. Menus can be associated with users and groups **with the condition** that the connection belongs to a certain Zone. This way it is possible to conditionally associate applications to users, based on geography, domain, or software versions just to name a few.

Here are the basic steps necessary to create and define zones.

Add Zones

Create Rules

Assign Zones to Groups

Adopt Devices (EDCs) and Assign Device (EDC) to Users

The Primary Interface consists of the EDC Admin Window in the Access Rules Manager program and several sub menus to view Access, Manage Identity Files and Assign/Lock Identity files to users. Most of these menu's are available when you "right-click" inside the Access Rules Manager main window.

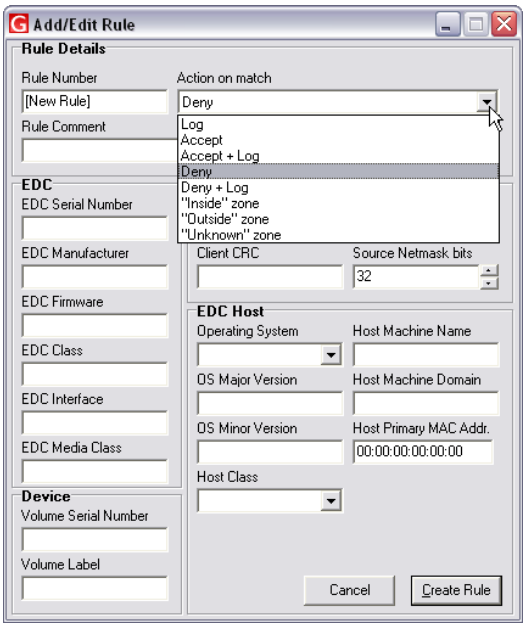
Copyright Giritech A/S 2009

Zone Types

There are many different ways to configure zones. Here are some examples of what is typically the most common types along with the associated levels of application access.

It's important to note that these are just examples, and that you should adjust access to align with your companies' internal security policies.

Inside or Inside USB: The Inside Zone should be used for company managed PCs. Clients falling into this zone will typically get access to the most comprehensive application menu and the ability to use their native clients.



Trusted: The Trusted zone is for access from clients that you trust, but where you don't necessarily manage their Computer. Typically, these are defined to be user specific from locations like Home PC's. In this scenario, you may decide to allow access to all the applications that are available in the Inside zone, however you restrict native client access and enable only Terminal Service usability without drive mapping.

Vendor or User Specific: Much like the trusted zone, this zone is typically reserved for clients that you trust but where you do not necessarily manage the computer or the computer is a native member of another domain. This is an administrator defined zone to enable specific access to a user or vendor specific list of applications.

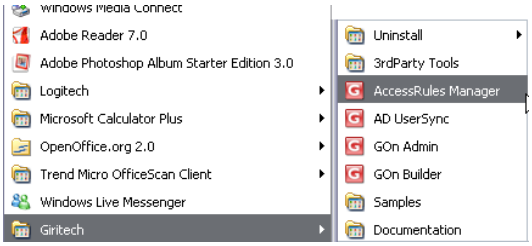
Outside: The Outside Zone is for users that are connecting from a client or a domain that you have no knowledge of. Typically, this could occur when users connect from clients at airports, conferences. In this scenario, would typically restrict both the level of application access to include only non-sensitive applications and the use of only a Terminal Server client.

Update: Update zone is useful when upgrading clients from previous versions of G/On. When using this zone, the users upgrade experience is automated.

Deny: The final rule in your list will be a Deny Access Rule. Clients that do not match any of the defined zones will match this zone and be denied access.

Copyright Giritech A/S 2009

Setting up Zones

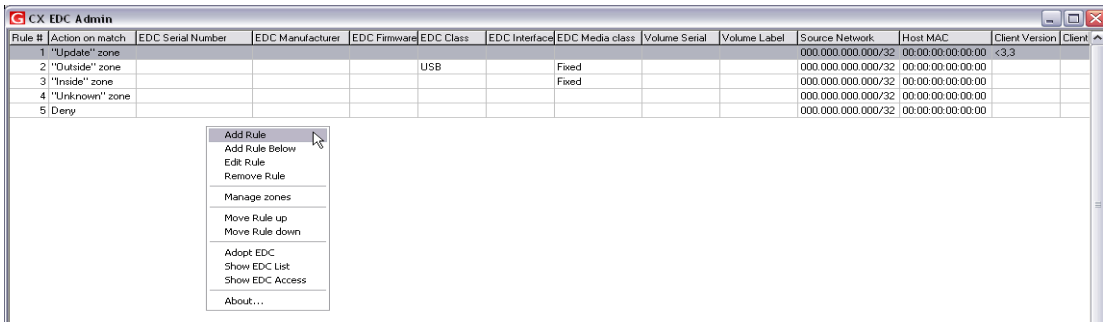


1. **Start the G/On AcessRules manager (CXRulesAdmin.exe)**
2. **Logon with the username and password that you defined in G/OnBuilder (Master or sub)**

Note: To use the validation rule zones and features in the AccessRules Manager, you must have checked the "Enable Ruleset Validation Engine" feature on the G/On Builder User Directory Tab.

After you enter your password, you will be presented with the CX EDC Admin window.

3. **Right Click on the CX EDC Admin Window and select one of the following options**


CX EDC Admin
Rule # | Action on match | EDC Serial Number | EDC Manufacturer | EDC Firmware | EDC Class | EDC Interface | EDC Media class | Volume Serial | Volume Label | Source Network | Host MAC | Client Version | Client
1 "Update" zone 000.000.000.000/32 00:00:00:00:00:00 <3,3
2 "Outside" zone USB Fixed 000.000.000.000/32 00:00:00:00:00:00
3 "Inside" zone Fixed 000.000.000.000/32 00:00:00:00:00:00
4 "Unknown" zone 000.000.000.000/32 00:00:00:00:00:00
5 Deny 000.000.000.000/32 00:00:00:00:00:00
Add Rule
Add Rule Below
Edit Rule
Remove Rule
Manage zones
Move Rule up
Move Rule down
Adopt EDC
Show EDC List
Show EDC Access
About...

Add a Zone Rule

Edit/Move or Remove Rules

Manage Zones

Adopt EDCs

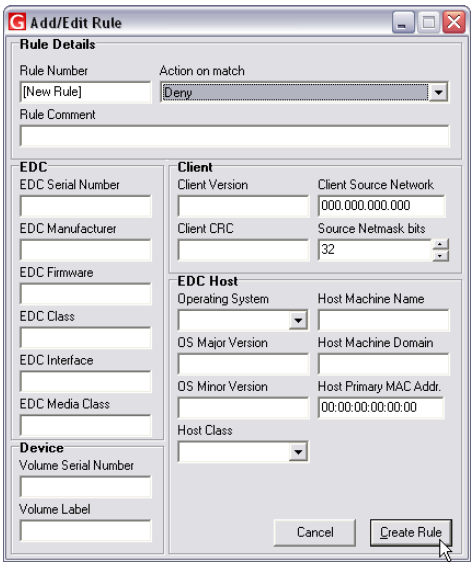
Show Adopted EDCs

View EDC Access

Add or Manage Zones

There are some default rules included in the basic G/On installation. But you should use this if you want to Add a new Zone or Edit an existing Zone name.

1. **Follow the directions in "Defining your own zones" to fill out the "Add/Edit" Rule Window.**



Defining Your Own Zones

1. **To Create a Rule, right click in the CX EDC Admin window and select Add Rule.**
2. **Consult the examples below to complete your Zone configuration**
3. **When finished Click Create Rule**

Note:

All the fields in the Add/Edit Rule zone are designed to be Exact Matches, with the exception of the fields mentioned in the list below where relational operators are allowed.

In these fields you can use the notations for "Less than" **(<),** "Greater Than" **(>)** or "No Match/Not Equal" **(!)**

Zone rule fields allowing relational operators:

- EDC Serial number
- EDC Manufacturer
- EDC Firmware
- EDC Class
- EDC Interface
- EDC Media Class
- Device Volume Label
- Device Volume Serial Number
- Client CRC
- Machine Name
- Host Class
- Client Version (not string comparison)
- Domain Name

Example: if the device is USB and the domain is "giritech.com" then it is trusted, but if the device is USB and the domain is "***!***giritech.com" ("not equal to

giritech.com") then it is not trusted.

Examples of Zones:

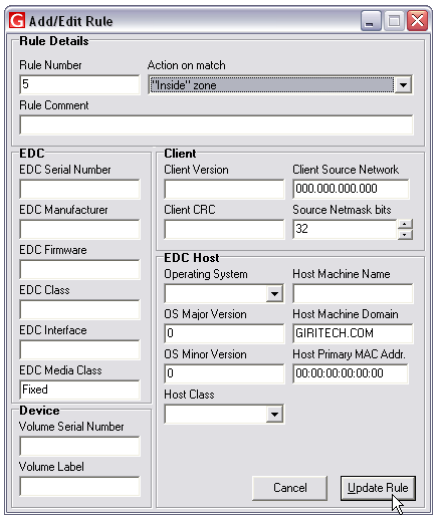
In this section, we have illustrated the most common zone definitions you will need to configure in your G/On Installation.

Each Example highlights the fields that must be populated in order to make the zones operational.

Some zones are by default included in the Action on Match drop down field. If you need to create a new zone, refer to the section above Adding and Managing Zones for instructions on how do define a new Action on Match item.

Defining an Inside Zone

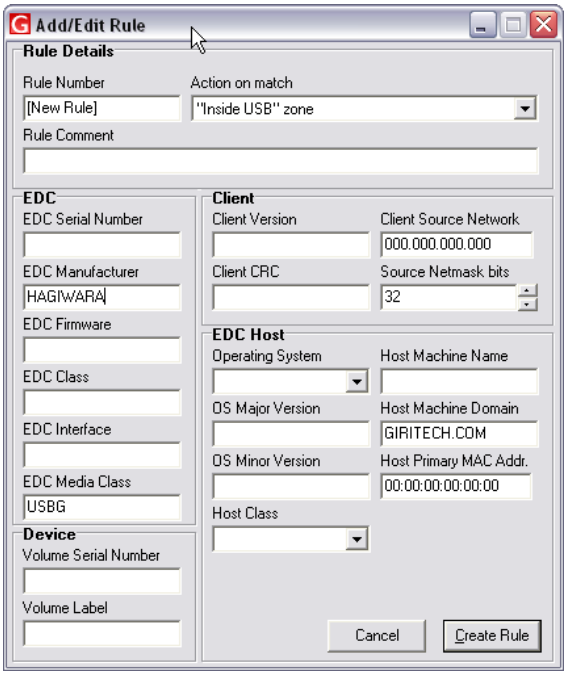
Inside Zones can be assigned to computers that are issued and maintained by your company.



Example Settings for Inside Zones using Desktop Clients:

Host Machine Domain (should be edited to reflect your company's domain)

EDC Media Class should be **Fixed**



Example Settings for Inside Zones using USB Clients:

Host Machine Domain (should be edited to reflect your company's domain)

EDC Media Class : USBG

EDC Manufacturer : HAGIWARA

Note that the EDC settings can be used as standard as they refer to G/On's unique USB Keys.

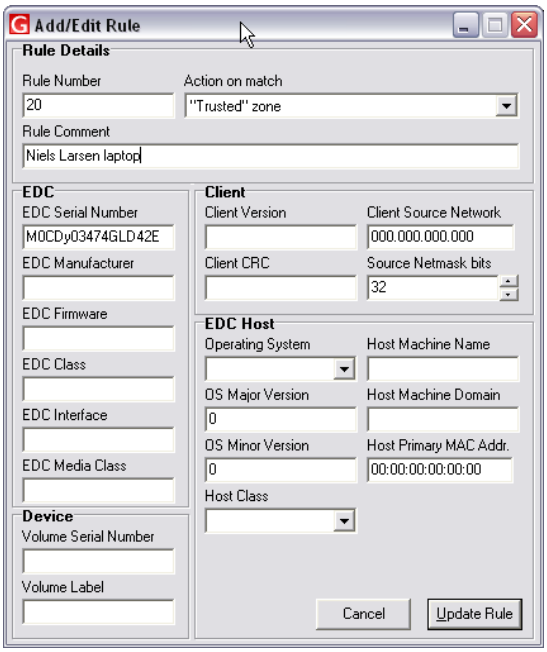
In the examples above the rules assume that the computer is a member of the GIRITECH domain. So when the user is using a computer that is from the Giritech.com domain, it will be assigned to the *inside* zone.

Because we created 2 rules, one for desktop client and a second for USB Clients, all users on Giritech.com domain laptops receive the same menus.

Clients with the USB Keys can also connect from non-Giritech domain computers, but would be placed into an “Outside Zone” and receive a different menu as they will not match the Giritech domain. (See example on Outside Zone below).

Defining a Trusted Zone

Under certain circumstances you may have trust for the user, but not necessarily manage the computer that they are connecting from. An example could be an employee on their home computer or a trusted vendor from another company.



In these cases you would want to create a trusted zone that allows more access than an Outside zone, but more restricted than if they were on a corporate managed computer.

Example Settings for Trusted Zones:

Assign An EDC Serial Number

Describe the Rule in the Rule Comment Field

We can also assign this EDC to the user by assigning an owner or locking the EDC as defined on page 55, “Manage EDCs”.

Defining a User or Vendor Zone

It is also possible to create a Zone rule for specific users. These rules allow the Administrator to provide a unique menu or zone for an individual user or vendor. They are very similar to Trusted Zones, however to ease administration, you should create a different zone name.

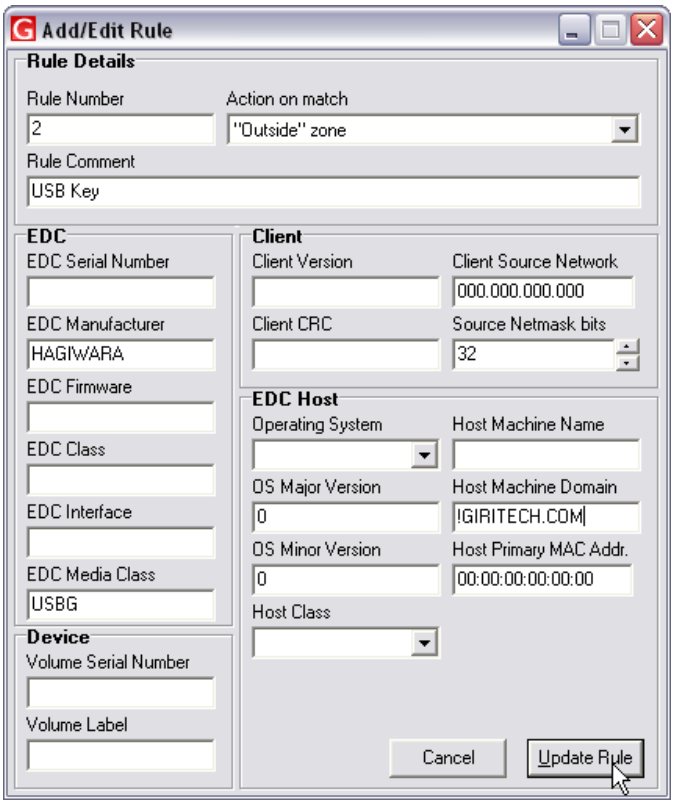
Example Settings: If you have an external vendor that books meetings for you or do your monthly book-keeping. You would want to

1. **Add a zone with the Name of the Vendor or User**
2. **Create a new Rule that enables this zone.**
3. **Add the EDC Serial Number from this User**
4. **If you want to further restrict the location from where they access you can choose to enter the Host Machine Domain field.**
5. **If the Vendor is using a USB key, you may want to use the standard EDC settings used in the previous example.**

Copyright Giritech A/S 2009

Defining an Outside Zone

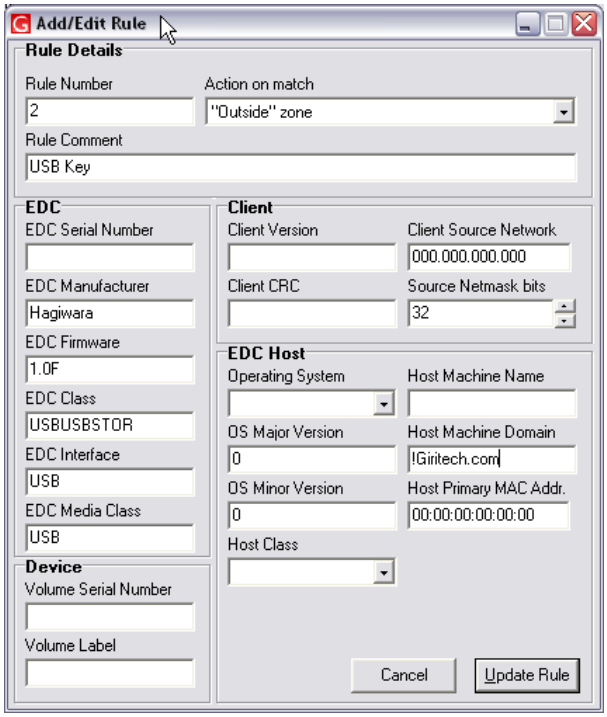
Outside Zones should be assigned to computers that are not issued or maintained by you.



Example Settings:

- Host Machine Domain (should be edited to reflect your company's domain and use "!" proceeding the domain name to reflect Not Equal To. The format should look like this: *!domainname.com*
- EDC settings – The settings used in this example can be copied as standard.

In this scenario if the user connects with the USB key on a Non-Giritech domain machine the Outside zone rule would be in effect. This is because Host Machine Domain would fail and the match on the G/On USB would pass, directing the user to the OUTSIDE ZONE rule.



Important Changes to Zone Rules for USB Keys when upgrading from pre-3.3 G/On

As of Version 3.3 and onwards, you need to review Zone Rules that Apply to USB Keys

The Standard EDC Format has changed. For users upgrading from versions of G/On before 3.3, there is a rule update that will convert your **EDC Media Class** value from CDROM to the new USBG. This happens automatically when you update your database as a part of the step 4 in the "G/On Builder Changes during Upgrade" (page 43).

For security purposes, you should review all your zone rules for USB Keys and change the values for **EDC Manufacturer** to HAGIWARA and **EDC Media Class** to USBG. Unless you are using a specific **EDC Serial Number**, then other fields like **EDC Firmware**, **Class**, and **Interface** should be blank.

*Note that **Volume Label** under **Device** will change on USB key's depending on whether you are accessing the ReadWrite or Read/Only partitions. This field should therefore not be used in standard zone definitions for USB keys.*

Copyright Giritech A/S 2009

Defining an Upgrade Zone

To define an upgrade zone you need fill out the Client Version field.

1. **In the client version field enter the name of the version number you want to upgrade all clients to.**
2. **You can choose to denote it as (examples):**

All clients less than the version number: <3.3.0.915

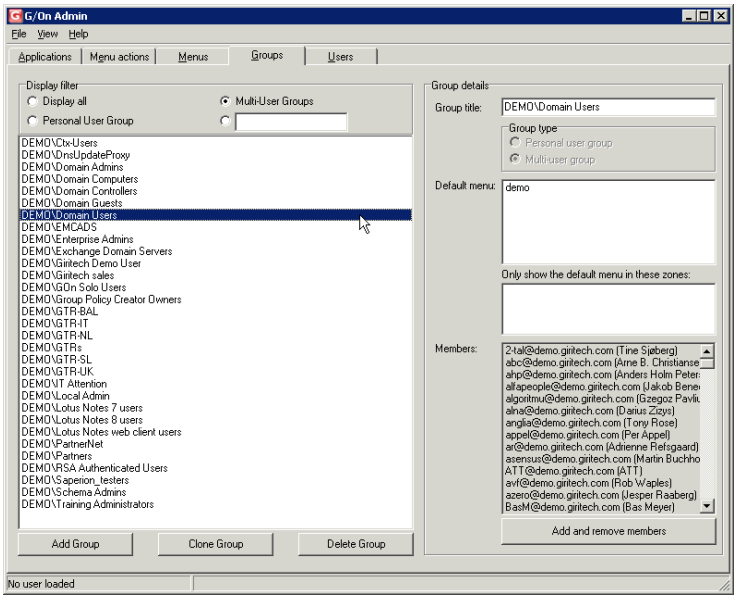
To downgrade, you could use: > 3.3.0.915

Or anything that is not equal to this version !3.3.0.915

3. **Now proceed to the section on Application Strings, Configuring G/Update in Chapter 6.**

Assigning Zones to Groups

Once you have defined all your zones. You will need to assign the Default Menu available to users in each defined zone.



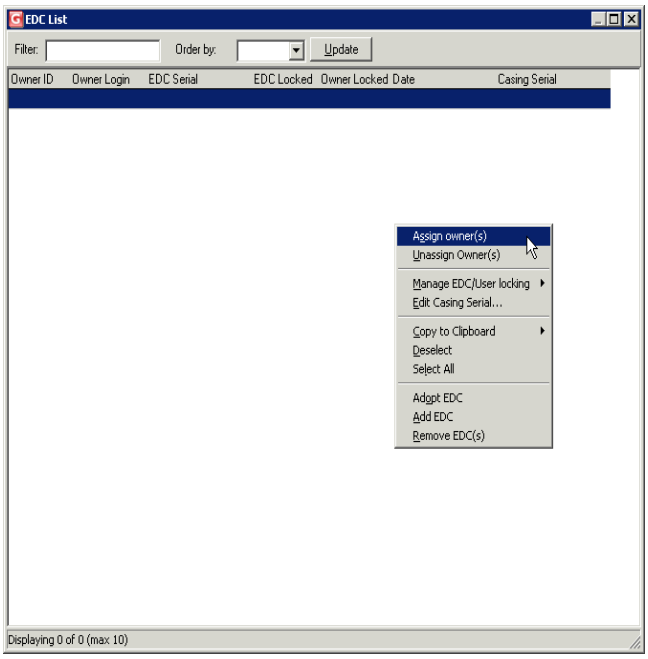
To complete this process you should

1. **Go to G/On Admin, (see chapter 6) press F3 and Log onto G/On Admin as Administrator.**
2. **Select the Groups Tab in G/On Admin.**
3. **Select the User Group**
4. **Select Which Menu Item should be available**
5. **Highlight the zone or zones where it should appear.**
6. **Repeat this process for Every Zone you have defined.**

In this example, all Enterprise Administrators that are logging on from a client that matches the Inside Zone, will receive the menu item “Applications”.

More information on defining applications, menus and applying zones to groups or users is covered in Chapter 6.

Manage EDCs



To manage an EDC, right click anywhere in the “Show EDC List” window in the Access Rules Manager. Then, right-click any EDC listed in the EDC List Window and select the appropriate action from the drop down list.

Here you have the options to:

Assign EDCs to users: Officially assigns responsibility of the EDC to a named user.

Lock Owner: If you lock the owner, then the user can only use this EDC and no other EDC. However many users can still be configured to use the same EDC!

Lock EDC: This EDC can only be used by this person thus disabling any other user from using this specific EDC.

Edit Casing Serial: this entry allows you to enter the external serial number that is laser engraved on the USB keys and associate it with the internal unique ID of the key that only the G/On system can read. This eases administration of lost key’s as they can be associated with user profiles using the external ID on the key without jeopardizing the security of the internal serial ID.

Adopt/Add/Remove EDCs. Adopt new EDCs that has tried to contact the G/On Server or manually adding new EDCs. Removing EDCs that needs to be locked-out from the G/On server.

More information on assigning and managing (EDCs) is covered in Chapter 8: Adopting Users. Note that some of the EDC management operations can also be performed from within **G/On Admin**.

Copyright Giritech A/S 2009

Chapter

6

G/On Admin

G/On Admin is your primary tool for defining and configuring your applications, menus and managing your users.

The Admin tool is your primary interface from everyone conducting routine helpdesk tasks to Senior Network Administrators that are responsible for remote connectivity to applications.

The G/On Admin is the tool you will need to use to:

Import Users and Groups from your Active Directory

Create Application Connectivity Strings

Create Menus

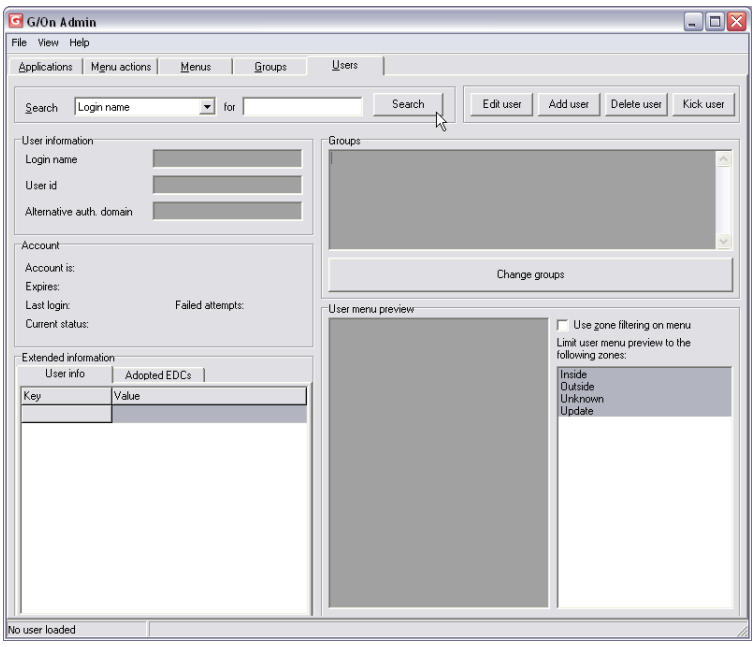
Create Groups and Users

Assign Users and Applications to Users and Zones

The Primary Interface consists of two drop-down menus and five tabs which you will use during the configuration. The next sections will walk you through the necessary settings for the:

- **Applications Tab**
- **Menu Actions Tab**
- **Menus**
- **Groups**

User Management is explained in Chapter 7.



Basic Concepts that are used in G/On Admin

Application string: This is the most basic element in the EMCADS system. An application string is a sort of application specific *template* used to launch applications and programs on the client and manages the secure G/On connection between the client and the server. Application strings can contain a series of changeable parameters separated by semicolons.

Action type number: A simple integer that indicates what kind of action should be executed on the client and how the following parameters should be interpreted.

Menu actions: A menu action is an application string that has been completely configured. A menu action contains fixed parameters such as server name, application path and port numbers. Menu actions are basically representations of the command-line commands executed when selecting one of the items on the user Menu.

Menu: A menu is built using a series of Menu Actions. A menu is a simple, hierarchical tree structure common to most Windows programs. The final menu that is displayed for the end user may contain several menus, depending on group relationships and zones.

Group: A user group can contain one or more users. A personal user group is always created when a new user is created (or imported). A group can have a default menu assigned to it, meaning that all members in this group will get this menu on login. If a user is a member of more than one group, the user will get a menu containing the combined contents of the menus assigned.

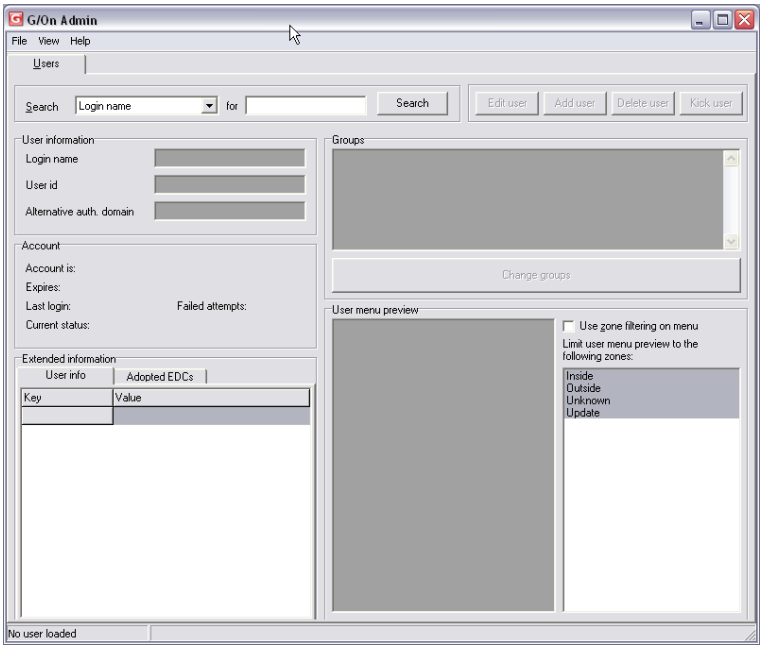
User: A user can be a member of multiple groups, but is at least a member of their own personal group. (This is the one group they cannot be removed from). The menu that the user is assigned is based on the groups they are member of. It is possible to attach detailed information about each user.

Zones: User Groups can be assigned Zones as a way to manage menus (and hence application access) depending on the active zones for each user. Refer to chapter 5 for details on Zones.

Copyright Giritech A/S 2009

Getting Started as an Administrator

From the start menu > All Programs > Giritech select GOn Admin, to launch the G/On Admin tool. Access rights are controlled by the AD and users must be logged on the server or in a terminal session that allows access to the G/On Admin application.



Administrator access requires the additional password that was configured during the G/On Builder installation and configuration process. Press F3 or choose "Administrator mode" from the File menu to enter administrator mode in G/On Admin.

Note: If you did not enter a username and password in G/On Builder the defaults are:

Username= admin

Password= Password

Defining Administrator Levels in G/On Admin

Access to the different tabs in G/On Admin's advanced functionality directly corresponds to the group levels as they are defined in the AD.

The two additional groups can be added to the AD and relevant technical personnel can be assigned to any group in AD, that ends with:

- Helpdesklevel1 (Ghotline1) – basic user/menu management
- Helpdesklevel2 (Ghotline2) – advanced user/menu management

For example: membership of a group called GiritechGhotline2 gives the user GHotline2 rights.

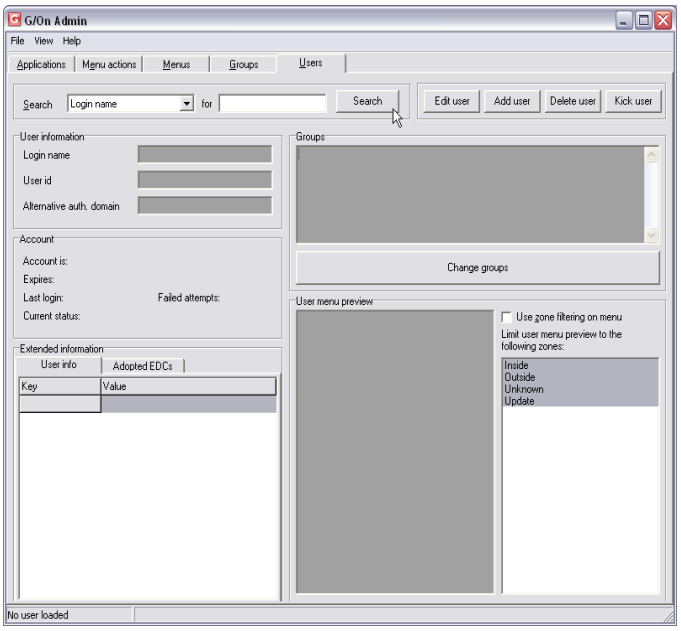
Copyright Giritech A/S 2009

Administrator Access Overview

User Administration Tab

Administrator Level: All Admin Users

- ❒ View user account information.
- ❒ View access zone information
- ❒ View user menu profile
- ❒ View adopted EDC's (Electronic Data Carrier like USB device or host PC)
- ❒ No edit or delete functions are available at this level.



Group & Menu Tabs

Administrator Level: Helpdesk level 1

Users at this level inherit the User tab, but have access to the Group and Menu tabs. At this level staff can:

- ❒ Add & remove members from groups
- ❒ Disconnect Users
- ❒ View Online Users
- ❒ Adopt unknown EDCs (EMCADS Data Carrier (EDC) USB device or host PC)
- ❒ Create Groups
- ❒ Reset user logon after lockout
- ❒ Assign a default menu to each group
- ❒ Lock default menus to zones
- ❒ Assign defined actions to menus

Menu Actions Tab

Administrator Level: Helpdesk level 2

- ❒ Edit, create and delete already created menu actions

Applications Tab

Administrator Level: Default Administrator mode

Professionals in this category are typically senior level operations staff that are tasked with the strategic deployment & maintenance of the corporate infrastructure or Giritech Certified Partners. The applications tab in G/On Admin is where application connectivity occurs. Staff at this level can:

- ❒ Utilize the Application creation wizard
- ❒ Application string creator
- ❒ Define Zones
- ❒ Sync AD
- ❒ Adopt EDC from file (USB specific)
- ❒ Perform backup/restore operations on the database

Copyright Giritech A/S 2009

File Menu

Administrator mode
Switch to administrator mode by pressing “F3” or select “Administrator mode” from the “File” menu. You will be prompted for the G/On administrator username and password.

Note: If you did not set a password in G/On Builder, the default is Admin/Password – capital “P”.

Maintain Zones
Here you can add or remove names of Zones. To *define and create* Zones go to the AccessRules Manager.

Adopt Unknown EDCs
This takes you to a window that shows connection attempts from unknown EDCs that has the Identity file of the G/On server and has tried to contact the server using this file. The list is sorted chronologically. Right-click on a list item to adopt an EDC.

Adopt EDC from file
Provides you with the option of adopting all the delivered keys, by importing the file EDCSERIALS.DAT, which is on a specially marked G/On USB key when delivered from Giritech manufacturing.

Sync AD
Invokes USync.exe from the EMCADS server directory (see next section). This imports (changes in) AD users and groups to the EDMS based on the parameters setup in G/On Builder. See below.

Backup/Restore
See Chapter 11

Online Users
See Chapter 7

Synchronize Active Directory

Active Directory synchronization uses the G/On tools USync or AdSync. Both tools get their primary settings from the “AD Sync” Tab in G/On Builder but also need configuration files to operate correctly.

Warning:

USync and AdSync are *not* compatible and should therefore *never* be used on the same installation. The following describes how to transition from a USync installation to an AdSync installation. It is important to remain with AdSync after the transition.

USync is the default tool designed for smaller installations running on the internal EDMS. It is also USync that will be invoked when running Active Directory

synchronization from within G/On Admin under the File menu > Sync AD (or Ctrl+S).

AdSync is an advanced tool supported from G/On 3.4 and onwards that is designed to support larger complex installations running on MS SQL[EP] databases and with complex AD setups and many users. This tool has to be operated from the command prompt interface using configuration files as described below.

> **Note:**
>
> If you are not an experienced Windows and AD user then use the default USync tool. AdSync requires a deeper understanding of running from the command prompt under windows and a deeper understanding of advanced AD configurations to function correctly.

The end result from running either of the tools is however almost the same:

- All users from a chosen AD Security group are imported
- All Security groups of which these users are members are imported along with the membership information
- User information contains login name and some details
- Group information consists of the group name, suffixed by the NetBIOS name.

The differences are:

- USync imports only global and universal security groups. AdSync also import local security groups.
- USync imports all users in the domain. AdSync only imports groups in which one or more of the chosen users are members.
- USync only imports the “display name” of the users whereas AdSync also imports email, title, street address, zip code, company, work, home and mobile phone numbers.

The following sections provide configuration and operational details about the two tools.

Running USync

If you choose to use the Active Directory you should create a G/On Specific group and assign the users that will be G/On to that group.

Using the USync, your users are automatically imported from your Active Directory. When syncing users from AD with USync, only the Full_Name value is synchronized. All other values are must be manually added to the User Information tab.

For more information on How to manage Groups and Users synchronized from the Active Directory, see Chapters 6 and 7.

Using USync

Synchronization of your Active Directory can be:

Run manually by going to **G/On Admin> File > Sync AD**

Scheduled via the Command Line

To subscribe to changes in AD, schedule USync.exe to run, for example once every hour. This can be done by adding USync.exe to the list of Scheduled Tasks on the Windows server.

Using the Command Line to Schedule USync Tasks

C:\>SCHTASKS /Create /RU SYSTEM /RP runaspassword /SC HOURLY /MO 4 /TN USYNC /TR

"C:\Program Files\Emcads\usync.exe" /SD 23/10/2005

RESULT FROM INSTALLING A NEW SCHEDULED TASK:

INFO: The schedule task "USYNC" will be created under user name ("NT AUTHORITY\SYSTEM").

W**ARNING: Password will be ignored for "NT AUTHORITY\SYSTEM" user.**

SUCCESS: The scheduled task "USYNC" has successfully been created.

RESULT FROM EDITING AN EXISTING SCHEDULED TASK:

INFO: The schedule task "USYNC" will be created under user name ("NT AUTHORITY\SYSTEM").

WARNING: Password will be ignored for "NT AUTHORITY\SYSTEM" user.

WARNING: The task name "USYNC" already exists. Do you want to replace it(Y/N)? y

SUCCESS: The scheduled task "USYNC" has successfully been created.

TROUBLESHOOTING USYNC

USync can be run with command-line parameters, for troubleshooting purposes:

-d: Debugmode, outputs much more logging info than normal

-f: Flush, deletes all users and groups from the EDMS

-c <name>: Clean (delete) all users and groups from <name> domain

Alternatively there is a -? switch to bring up a "help" dialog with a list of the options

For more information on this Command line tool you can use one of the following:

SCHTASKS /?,	SCHTASKS /Delete /?
SCHTASKS /Create /?	SCHTASKS /Run /?
SCHTASKS /End /?	SCHTASKS /Query /?
SCHTASKS /Change /?	

Running AdSync

AdSync is the advanced Active Directory synchronization tool designed to support larger G/On installations with complex AD configurations. AdSync default only support MS SQL[EP] based G/On installations.

Note:

If you want to use the built-in EDMS database (or MySQL) you need to manually set up an ODBC connection to the G/On database and enter the name of this and other information in a separate configuration file. Note that this also means that AdSync does not work on encrypted databases. Therefore, in order to use AdSync, make sure that "Encrypt data" checkbox in the "User Directory" tab in G/On Builder is not checked.

Setup AdSync

This section describes how to configure AdSync.

Configuration file

A configuration file containing the configuration details should be created and put in the same folder as the AdSync program. By default the configuration file is assumed to have the name “AdSync.ini”. If you wish to use another name you should use the “inifile” option, specifying the file name, e.g.

```
AdSync.exe --inifile myfile.txt
```

A configuration file based on the data entered in G/On builder can be created by using the "dumpinifile" option, e.g.

```
AdSync.exe --dump_inifile myfile.ini
```

Note however that database information is not dumped.

In the following we will describe how to set up the configuration manually. First some typical scenarios are described. After that we give a full description of all options available.

Typical configurations

In this section we will describe some typical scenarios and give examples on how to configure AdSync for each of them. Database setup is the same for all of the scenarios and is described last.

Single domain

If you have a single domain setup the user account used for running AdSync must be logged into this domain. You therefore only need to specify the name of the group from which users should be drawn.

Example:

```
[AD]

Emcads group = Domain Users
```

Multiple domains

If you have multiple domains, there are two different approaches to choose from:

- Synchronize with each domain separately

- Synchronize all domains together

Note that the second case is only possible if you can add users from all domains to a group in the domain you are synchronizing from.

Synchronizing with each domain separately

In order to synchronize with several domains you must add a domain section to the inifile for each of the domains. Each domain section has to have a unique name starting with "Domain" and must contain the option "DNS Name".

Example:

```
[AD]

Emcads group = G/On access group

[Domain 1]

DNS name = mydomain.com

[Domain 2]

DNS name = myotherdomain.com
```

In this example the name of the Emcads group is the same in the two domains. It is however possible to specify another name in each "Domain xxx" section, which then overrides the one specified in the "AD" section:

```
[AD]

Emcads group = G/On access group

[Domain 1]

DNS name = mydomain.com

Emcads group = Domain admins

[Domain 2]

DNS name = myotherdomain.com
```

Synchronize all domains together

Instead of maintaining a group for G/On access in each domain it could be more efficient to maintain one universal group containing users from all of the domains. In order to synchronize data in this setup your inifile could look like this:

```
[AD]

Emcads group = G/On access group

Domain local only = False
```

This configuration assumes that the user account used for running AdSync is logged into the domain containing the "`G/On access group`" group. Setting the "`Domain local only`" option to False ensures that entries from other domains are imported as well.

If the domain containing the "Emcads group" is part of another domain than the one the user account is logged into, then you simply add the domain in question in a domain section:

```
[AD]

Emcads group = G/On access group

Domain local only = False

[Domain]

DNS name = mydomain.com
```

Note that the "`Domain local only`" option also can be specified a "Domain xxx" section in order to override the value specified in the "AD" section. This is, in fact the case for all options in the "AD" section.

Database setup

If the database connection information in G/On Builder is valid for AdSync, i.e. the database is SQL Server, you don't need to specify anything regarding the database in the inifile.

You can however override or change these settings in the inifile.

Example:

```
[Database]

NT Authentication = False

Username = user

Password = password
```

Here the database connection will be made using the given user name and password instead of using NT authentication.

There is also the possibility of using an ODBC connection to connect to the database.

Example:

```
[Database]

ODBC Source = emcads odbc
```

If the "ODBC Source" option is set, it overrides any other database connection settings. You can also specify a username and password for the ODBC connection:

```
[Database]

ODBC Source = emcads odbc

Username = user
Password = password
```

All configuration options

This section describes the full set of options available. Note however that most cases are covered by the typical configurations described in the previous section; so much of the information here may not be relevant to you.

The configuration file contains the following sections and values:

```
[AD]

Emcads group=EMCADS
```

Emcads group: the name of the group containing users to be synchronized. If not specified the name "EMCADS" is assumed.

Domain local only: Specifies whether users and groups outside the domain should be imported. This option can be used to set up synchronization of multiple domains in one go. Possible values: True/False. Default value is True

Delete unmatched entries: Specifies whether to delete a user or a group in the database, if it is not found in Active Directory. Possible values: True/False. Default value is True

Force update: A "last changed" timestamp is saved along with each Active Directory object in the database. This timestamp is used to check whether an object needs to be updated. This option overrides this check and updates all data. It could be useful if someone accidentally changes some data for an AD user in G/On Admin.

```
[Domain xxx]

DNS Name = mydomain.com
```

DNS name: The dns (domain) name (e.g. mydomain.com). This option is mandatory.

Netbios name: Can be specified if you want to override the auto detected Netbios name. Should only be specified if users are having trouble logging in with the auto detected name.

All options from the "AD" section can also be specified here and will override settings for this domain only. This could for example be used for specifying domain specific emcads group names.

```
[Database]
```

Settings overriding the ones read from G/On Builder:

Host: The name of the database host computer.

Database : The name of the database to connect to on the host

Username: Database user name.

Password : Password for the user

NT Authentication : Whether to use NT Authentication or not

Other settings:

ODBC source: The name of an ODBC data source pointing to the Emcads database. This setting overrides other connection settings.

Encoding: The encoding of the Database.

Transaction size: Can be set if saving to the database is time consuming. Some databases (e.g. the built-in database) perform better if updates are made in larger transactions. The default size is 1.

```
[Debug]
```

Add this section in order to get debug log output.

Running AdSync

To run the tool, open a command prompt at the folder containing the AdSync executable and the configuration file. In the prompt type:

```
AdSync.exe
```

and the synchronization will begin.

You can also schedule the task to be run with the Windows Task Scheduler or similar tools (see under USync for more details).

Data imported with USync – transitioning from USync to AdSync.

AdSync will check whether data imported with USync is present in the database. If this is the case it will abort. In order to upgrade data imported with USync, AdSync must be run in a special mode. Here is a recommended recipe for transitioning the data:

2. Backup database

3. Open Command Prompt at Emcads folder and run "AdSync.exe --usync"

4. When command has finished with success, you should create a configuration file for AdSync by running the command "AdSync.exe --dump_inifile AdSync.ini"

5. Synchronize again by running "AdSync.exe" and verify that it finishes without errors.

Notes:

AdSync will match and convert all existing users and groups which were synchronized using the USync program. If AdSync finds one or more users, which it cannot match it will print a list of the users in question to the log and stop. If these users should be deleted (from the Emcads database) then you can run the command again with the extra option "force", i.e. "AdSync.exe --usync --force".

Otherwise you should run USync once and check again. If you still have the problem then please contact Giritech Support.

When AdSync is run with the "usync" option it will automatically switch to debug logging. This creates an improved information base to assist in support cases. Please have this log available when contacting Giritech Support.

AdSync has a "readonly" option, which, if specified, has the effect that no data is saved to the database. This can be used for testing an upgrade before actually doing it.

Command line options

AdSync has a number of command line options for performing other tasks and/or configure the way the tasks are done. These options are described in this section.

All command line options should be given on the form "--<option name>", e.g.

```
AdSync.exe --export
```

Some options can be activated using one letter abbreviations. Use option "`--help`" to see available options.

Task options

In this section we describe options to AdSync which changes the functionality to perform specific tasks. If none of these options are specified, a normal synchronization is done.

clear

Delete all users and groups belonging to the domain(s) specified in configuration file

export

Export data from AD without entering it into the database. The data from each domain specified in the configuration file is exported to an XML file named `<dns name>.xml`, e.g. `mydomain.com.xml`. The resulting file(s) can be imported using the *import* option.

Example:

```
AdSync.exe --export
```

help

Show list of available options and exit

import

Import data from a file exported with the *export* option.

Example:

```
AdSync.exe --import myfile.xml
```

usync

Convert data imported with USync to format recognisable by AdSync

version

Print product version and exit

Other options

delete_unmatched

Setting this option will override any "Delete unmatched entries" settings in the configuration file.

force

With "usync" option set:

During upgrade of data imported with USync, AdSync may encounter users which it cannot find a match for in Active Directory. Normally this will cause AdSync to halt, but setting this option will result in the removal of the unmatched user(s) and the upgrade will continue.

Without "usync" option:

AdSync will not run if it detects that the database contains data synchronized with USync. This option forces AdSync to run even if this is the case. Using this option is not recommended unless you are an expert user. *AdSync and USync are NOT compatible*. If you have imported data with one of the tools, then synchronizing with the other will not work correctly, i.e. some data may be deleted and groups and users may appear more than once in the G/On admin module.

Example:

```
AdSync.exe --force
```

inifile

Run AdSync with the specified configuration file.

Example:

```
AdSync.exe --inifile myfile.ini
```

password

Password for database connection

readonly

Run in read-only mode, i.e. nothing is saved to the database. Useful for testing the result of a configuration.

username

Username for database connection

Logging in AdSync

Progress and other information is logged to the screen and to a log file called "AdSync.log", located in the same directory as the executable. Note that information is always appended to the log file, so you may want to delete this file regularly in order to avoid disk space problems.

Event log

Errors and warnings issued during execution of AdSync will be entered into Windows Application Event log. This enables you to get notifications about problems during execution, which can be useful if you are running AdSync as a scheduled task.

Debug logging

As mentioned previously, a special debug option is available. When running in debug mode, more detailed information is logged. You should only turn this option on for troubleshooting purposes, as it will decrease performance and cause the log file to grow rapidly in size. Note that when "usync" option is chosen, debug option is automatically set. The reason for this is that this option only should be used one time and if something goes wrong it simplifies the troubleshooting greatly, that as much information as possible is present,.

Recommendations for special cases

The simplest way to use AdSync is if you can run it on a computer which is logged into the AD domain and has a connection to the database. For security or other reasons this may not always be possible.

If it is not possible or convenient to have an AD account and database connection on the same computer, the only possibility for using AdSync is via the import/export options. You can export data on any computer which is logged into the AD and then transfer the exported file to a computer where you have set up a connection to the database (it could be the database server itself) and then import the data. Note however that the data in the export file is not encrypted in any way, so you may want to protect the file in some way, if you transfer it on an insecure line.

If G/On should be synchronized with more than one AD, without trust between them, these options are available:

Use a "Run as" approach

Create a user account for each AD that need to be synchronized and run AdSync as each user.

Distribute AdSync

AdSync can be distributed to a computer on each AD you need to synchronize with and then run on each of these computers. Note however that this requires that you can setup a connection from each of these computers to the G/On database. Note that there is no conflict in synchronizing several AD's at the same time, since the data is separated by the domain names. It is however still not recommended to do so for performance reasons.

Import/export

You could also use the import/export options as described above. This can be done using either approach described.

It depends very much on the local setup which of these options you should use. From a performance perspective, the tests we have made do not show any performance issues with remote AD or database connections. This is however strongly dependent on the network performance.

Troubleshooting AdSync

Below are listed some problems that may occur and suggestions for solving them:

```
dbi.operation-error: [Microsoft][ODBC Driver Manager] Data
source name not found and no default driver specified in
LOGIN
```

Cause: The ODBC connection could not be found

Solution: Check that the name specified in the configuration file under "ODBC source" is a valid ODBC connection.

```
dbi.internal-error: [Elevate Software][DBISAM] Invalid
SQL data type in input-binding
```

Cause: Missing or wrong database encoding string in configuration file

Solution: Add encoding option value in configuration file ("ISO-8859-1" is standard Latin encoding)

```
dbi.internal-error: [Elevate Software][DBISAM] DBISAM
Engine Error # 10498 Insufficient rights to the table
'tbl_user', a password is required in EXEC
```

Cause: The database is encrypted.

Solution: Uncheck the "Encrypt data" checkbox in the "User Directory" tab in G/On Builder.

```
dbi.program-error: [Microsoft][SQL Native Client][SQL
Server]Invalid object name 'tbl_user'. in EXEC
```

Cause: The default database for the ODBC connection is not the Emcads database. Note that by default an ODBC connection for SQL Server is set to connect to the "master" database.

Solution: In the ODBC connection configuration, make sure the default database is the Emcads database.

```
dbi.program-error: [Microsoft][SQL Native Client][SQL
Server]Invalid column name 'user_external_id'. in EXEC
```

Cause: You are using a G/On version prior to 3.4. AdSync only works for version 3.4 or later.

Solution: Upgrade to latest version of G/On (3.4 or higher).

Overview of G/On Application Connectivity

At the heart of G/On is the ability to extend connectivity to defined applications. Extending Applications is enabled by creating and configuring Application Strings.

To implement a connection to an application using G/On, you either need to understand how the application communicates over the network or use the built in Application String Creator which will define the standard application strings for you. An Application String is basically an action number with parameters that details the desired action on the client.

G/On addresses all Client/Server applications that connect to a fixed IP number (or DNS name), on fixed ports.

G/On supports TCP and UDP connections.

On the client side, G/On uses the loopback 127.0.0.2 as the listening address.

In the next section there is an overview of the most common settings and how to change them. **Chapter 12** provides a more detailed explanation.

Advanced Application Connectivity: What is a String

Strings are created by the Application Creator. But if you choose to open and browse the raw strings or observe them in the viewing window, you will see a long list of %, values and Brackets. This section gives you basic knowledge about the actual make-up of a string, however we recommend that you use the standard strings from the Application Creator.

All parameters in the raw strings must be surrounded by percentage signs (%). A parameter can have a **series of basic values** to choose among later, specified in square brackets [ ]. For example, if you want to include a parameter defining whether or not to display fullscreen using the values true or false you could make it like this:

%FullScreen[False|True]%. Notice that the values are separated by a horizontal bar. To make a particular value the default value, trail with ",default".

Example: %FullScreen[False|True,default]%

Some parameters can be forced to hold a value. This means that when the menu action is created, it is mandatory that certain fields are filled in (i.e. they can **NOT** be left blank).

Example: %DOMAIN,mustedit,noblank%

If you need to use a “%” sign in the string (for instance for URLs, Java applications and similar) you can use the notation: %25,noedit% (25 is the ASCII character %)

Example:

http://tld.com/?value=John**%25,noEdit%**Doe will return:

http://tld.com/?value=John**%**Doe

Four Step Method for Defining and Configuring Applications

Step 1: Identify the Types of applications you would like to make available

Step 2: Create the application strings with the Application Creator

Step 3: Edit Application String Properties and Parameters

Step 4: Apply the settings to make your applications work in your environment.

Step 1: Identify your Application Types

❑ Step 1: Identify your Application Types

These are the Application String types in G/On.

Type 4: **Terminal Services Connector (9 parameters)** Using this version, Terminal Services can be launched with single sign on. (Note: If you don't desire single sign-on use a Type 8 with the mstsc.exe executable)

Type 5: Legacy Citrix Connector (9 parameters) Using this version, the ICA Desktop can be launched with single sign on.

Type 7: Change Password (No Parameters) Can be used to enable users to remotely change their password.

Type 8: Single Port Application Connector (11 Parameters) Used to launch applications that only require a single port to connect to the server. Some examples are: Microsoft Navision, Web Browser etc.

Type 9: Application Launcher (2 Parameters) Launches local applications with corresponding parameters. Can be used after launching a gateway.

Type 10: Multi-Port Application Connector (9 parameters) Used to launch applications that require two or more ports to connect to the server. Some examples are: Outlook, Citrix PN and G/On Help (special configuration).

Type 1: Show log Predefined standard item.

Type 2: About Predefined standard item.

Type 3: Exit Predefined standard item.

Type 6 and 11+: Reserved for future use

Copyright Giritech A/S 2009

Note:

The Type 10 application string has been extended to support G/On Help. The extensions are reserved for G/On Help and are therefore *not* supported in the G/On Admin application editor. If you try to force changes to a G/On Help string it will fail! *Please refer to separate documentation on how to configure and use G/On Help*.

Defining Application Strings and Menu Actions

Once you have completed Step One and identified the types of applications you would like to connect, you are ready to move on to steps 2 - 4.

- ❑ **Step 2: Use the Application Creator on the Applications Tab to create the application strings**
- ❑ **Step 3: Edit Application String Template**
- ❑ **Step 4: Apply the settings to make your applications work in your environment.**

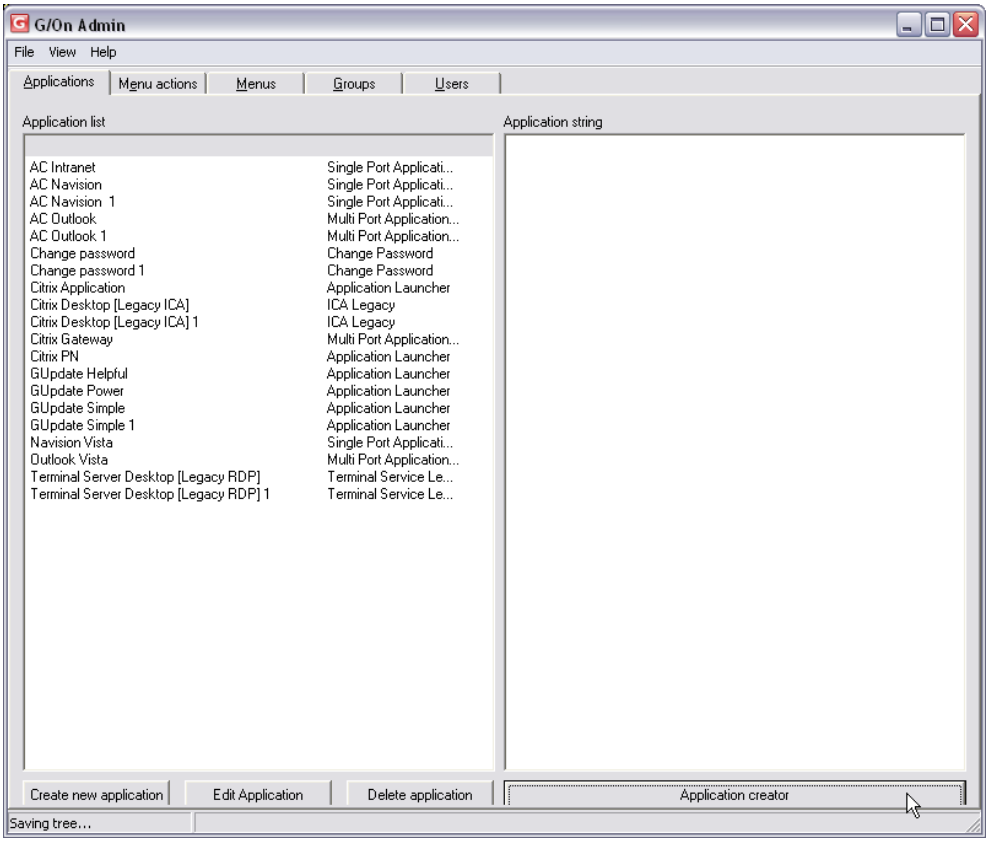
The basic overview of Steps 2 through 4 are included in the section below, more specific examples are included in the Application Connectivity Walk-Through section later in this chapter.

Step 2: Using the Application Creator

To define your Application Strings, use the Application Creator to create your Application String Template.

1. **Log onto G/On Admin as an Administrator**
2. **Go to the G/On Admin > Applications Tab.**
3. **Click > Application Creator button in the lower right corner of the window**

Select the Type of Application you want to create > Next or Done
Go to Step 3 to View the Application Template you have created.


G/On Admin
File View Help
Applications Menu actions Menus Groups Users
Application list
Application string
AC Intranet Single Port Applicati...
AC Navision Single Port Applicati...
AC Navision 1 Single Port Applicati...
AC Outlook Multi Port Application...
AC Outlook 1 Multi Port Application...
Change password Change Password
Change password 1 Change Password
Citrix Application Application Launcher
Citrix Desktop [Legacy ICA] ICA Legacy
Citrix Desktop [Legacy ICA] 1 ICA Legacy
Citrix Gateway Multi Port Application...
Citrix PN Application Launcher
GUpdate Helpful Application Launcher
GUpdate Power Application Launcher
GUpdate Simple Application Launcher
GUpdate Simple 1 Application Launcher
Navision Vista Single Port Applicati...
Outlook Vista Multi Port Application...
Terminal Server Desktop [Legacy RDP] Terminal Service Le...
Terminal Server Desktop [Legacy RDP] 1 Terminal Service Le...
Create new application
Edit Application
Delete application
Application creator
Saving tree...

Step 3: Edit Application String Template

In Step2, the Application Creator creates a template for your application string.

To open and edit the template that you created in Step2 go to:

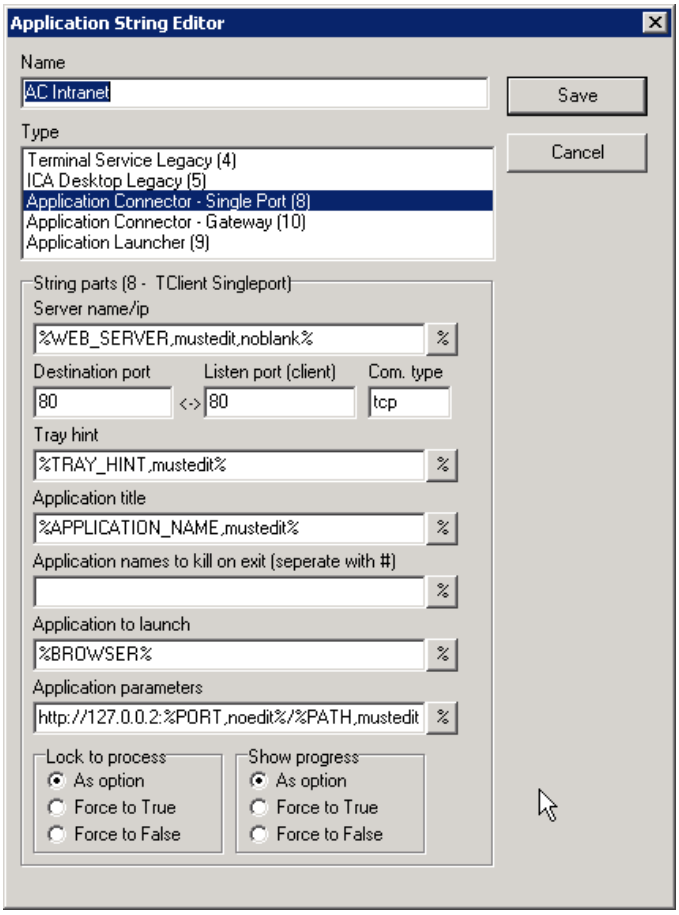
1. **G/On Admin > Application Tab**
2. **Highlight the Name of the Template you created with the application creator**
3. **Select Edit**

This will open the Application String Editor, which is your Template.

In the template, you will see that there are several Values that have been entered into your template.

Most of the values in the template are Generic, and are designed to Guide you on what values should be entered when you fill out Step4.

But some values are default parameters. As in this example, The Application to Launch is given as %BROWSER%



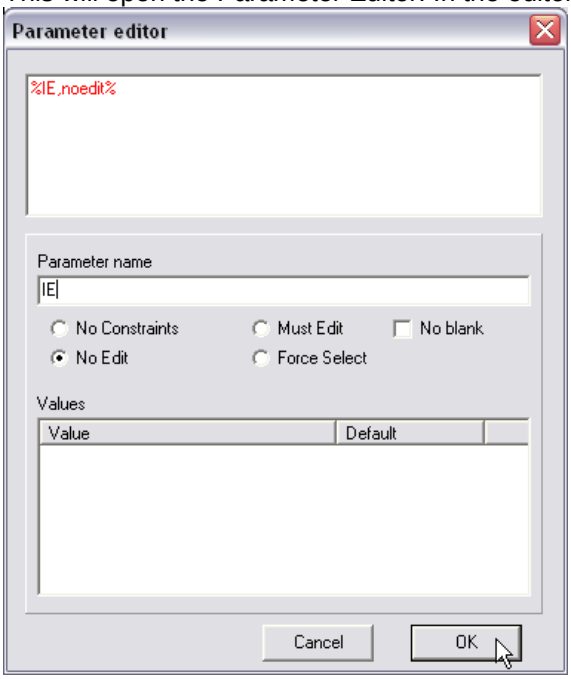
The %BROWSER% is a default parameter that creates a Full path to the PC's default Web Browser (e.g Firefox, Mozilla)

BUT if your corporate policy is to only allow use of Internet Explorer, you may want to change this value to read %IE,noedit%.

To change this parameter from %BROWSER% to Internet Explorer, you would:

> Click the % sign at the right edge of the field that contains the parameter you wish to edit.

This will open the Parameter Editor. In the editor:



> Type in the New Parameter Name, in this Case IE

>Verify that No Edit is Checked >OK.

> Verify that the new setting in the template reads %IE,noedit% and > click Save

Your template is now updated. You may now proceed to Step 4 to fill in the template.

Editing note:

For more information on other Default Parameters like %BROWSER% or %PORT%, consult the Default Parameters Table later in this chapter.

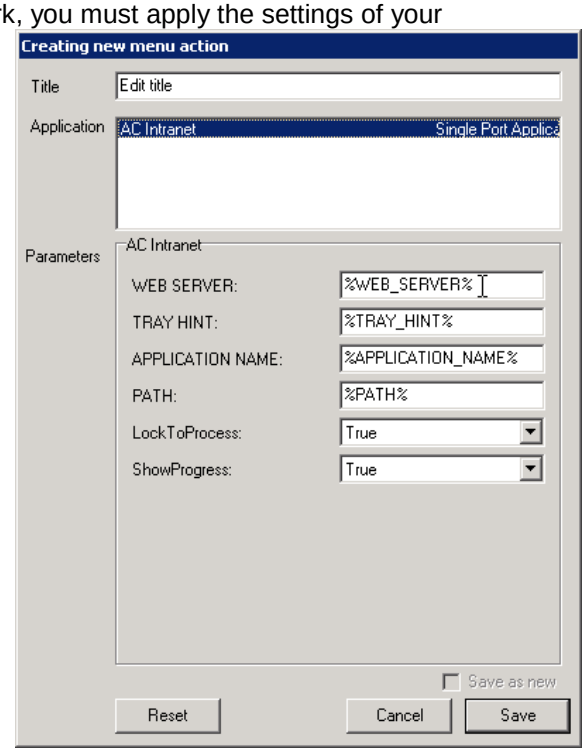
> **Note:**
>
> You can specify specific values directly in the Application String. However, by making them parameters, you have the option of targeting the string at more than one server and more than one company.

Step 4: Apply the settings to make your applications work in your environment.

Once you have viewed that the contents of your application Template are correct, you can proceed to the Menu actions Tab to fill in the Template.

>Go to G/On Admin > Menu Actions Tab

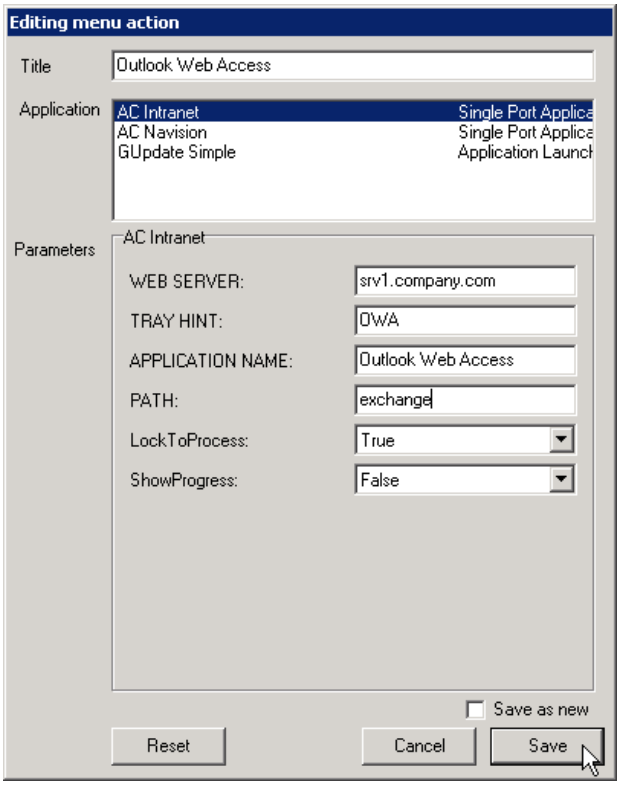
To get an Application String to work, you must apply the settings of your company's configuration to your template by creating a menu action. A **Menu Action** is the connector between the Application String and the menu that a user sees.



A menu action is used to target an application string to a specific server or application before it is added to a user group's menu.

>click the button: Create new Action > select the application template you want to fill in.

In this example, you see that you are prompted to replace the %SERVER_NAME% and other fields with the information specific to your company.



Here you should delete the existing text from the raw template and update the information with your company specific details.

Note: the server name should be the REAL name or IP address of the application server.

Copyright Giritech A/S 2009

Application Connectivity Settings Overview

To enable an application, there are a number of different variables you will be required to define. The table below defines the most common Application String Parameters that you will need to know to fully configure your applications in the Application string editor.

Field Name	Description	When to Apply	Can be use with String Types:
Application exe	Same as Application to Launch	When you want to run an application without setting up a port. For example: **notepad.exe**	Type 9
Application Names to Kill on Exit	These are the applications you want to have shut down when your main application closes	When your main application launches secondary applications you want closed with the main application. For example: Citrix often launches secondary applications.	Type 8 and 10
Application Parameters	The parameters you want to launch your application with	If launching notepad. This could be **Readme.txt**	Type 8, 9 & 10
Application Title	This is the Name you want to have your Application Identified by.	Typically the “Common” application Name. Such as: Outlook, Navision etc.	Types 8 & 10
Application to Launch	Same as Application.exe	When you want to run an application. For example: **notepad.exe**	Types 8 & 10
Autologin	Turns on Single Sign-On (SSO)	Can be use with Citrix and Terminal Services	Types 4 and 5
Communication Type (Com. Type)	Specify if the Application uses UDP or TCP	Consult your Application Guide to determine what type of communication is used	Types 8 & 10
Destination Port	This is the port that the Application Server listens on and the G/On server connects to	When your application server is listening on a port.	Type 8
Domain	Authentication Domain	Used to define what Authentication Domain should be used for Single Sign-On	Types 4 & 5
FullScreen	Forces the client to open as a full screen	Can be used with Terminal Services and Citrix	Types 4 and 5

	application		
Listen Port	Is the port, the G/On client should listen on.	Used with Single Port Applications	Type 8
Lock to Process	Locking to Process increases security.	Enabling it means that only the process started by this string can communicate through the G/On Connection on the Port that has been defined in the string.	Types 8 & 10
Map Drives	Maps Drives	Used with Citrix or Terminal Services	Types 4 & 5
Map Printer	Same as Map Drives	Used with Citrix or Terminal Services	Types 4 & 5
Ports to Forward	Multiple Ports to forward. These ports are the listen ports on the client as well as the forward ports from the G/On server to the application server	When your application is using more than one port	Type 10
Path	Part of the link in the browser link field, used to access virtual site of web server. Not required if the web server is setup to run a default site.	Examples: Here the web server is setup to run exchange as a virtual site. http://127.0.0.2/exchange in this case the PATH parameter = exchange. http://127.0.0.2/system/index.php another example of how to use the PATH parameter (system/index.php) http://127.0.0.2 – in this case the default web site on the web server is accessed	Type 8
Remote Application	Application to Launch	Use when you want to launch a specific application when running Terminal Services or Citrix. For example: A Terminal Services Outlook	Types 4 & 5
Server Name/IP Address	This is the Application Server Address	When your Application wants to contact the server.	Types 8 & 10
Tray Hint	This is the text that is displayed in the Windows System Tray	Use to enable your users to identify the application	Types 4, 5, 8, 9, 10
Window Resolution	This is the size of the application window	Use to control the size of the Terminal Server and Citrix Windows	Types 4 & 5
Show Progress	Activity indicator	Displays a progress window during operation	Types 8 & 10

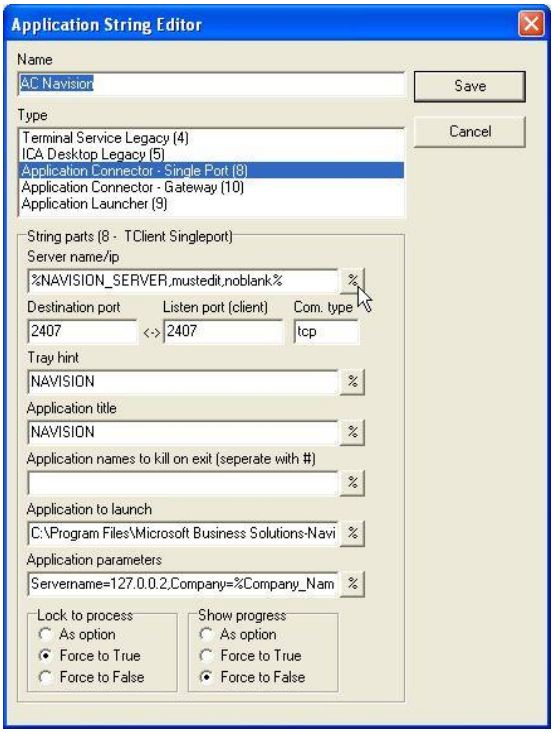
Application Connectivity for Native Clients

In this example, we will create a Template for Navision, edit it and create a Menu Action to connect to my Navision Application Server.

6. **All Application Strings are defined on the G/On Admin > Applications Tab. Click > Application Creator Highlight Application Connectivity > Next**

7. **Highlight the Application you want to Create > Done**

Go to G/On Admin > Applications Tab >Highlight the String You just created (in this example Navision) > Double Click



8. **Review the Settings and check that all information NOT contained within the "%" is correct.**

- ❑ **See the Application Connectivity Settings Overview Table for a complete explanation on the usage of each parameter.**

If you wish to review the parameters, click > % to open the Parameter viewer.

In this example, we verify that the Destination and Listening Port are correct and that the Tray Hint, Application Title and Path to the Application to Launch are correct.

In G/On, therefore, the application parameters, as seen in the example, will direct the Navision client to connect to a server that listens on 127.0.0.2:2407.

Copyright Giritech A/S 2009

Definition: Default Application String Parameters

The table below contains a list of Default Parameters that can be used when editing the G/On Applications Strings in Step3: Editing the Template.

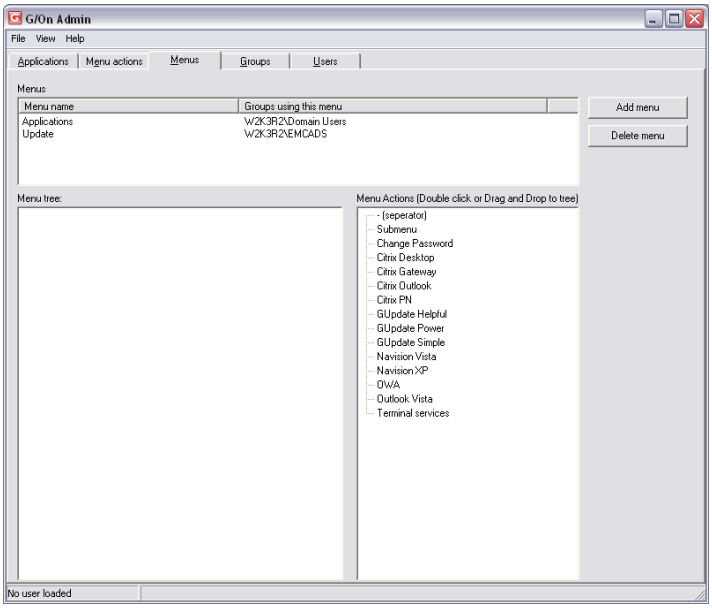
%USERNAME%	**The user's login name *exactly* as typed in the G/On login window (e.g "john.doe" or john.doe@enterprise.com or "ENTERPRISE/john.doe".**
%USER_LOGIN_NAME%	**The user's login name and domain association, e.g. "john.doe@enterprise.com"**
%USER_LOGIN_NAME_SHORT%	**Only the user's simple login name (e.g. "john.doe"), all domain information stripped.**
%GONPATH%	**The path to the drive and directory where the G/On Client is residing.** **On a G/On USB key, this is the Read/Only partition; on a PC with G/On Desktop Client installed, this is the directory where ECLIENT.EXE is launched from**
%DESKTOP%	**Path to the logged-in user's desktop directory**
%VENDORPATH%	**The path to the Read/Write partition on a G/On USB key. On a G/On Desktop Client, this is the Applications directory.**
%CLIENTDIR%	**Path to the eclient.exe. Left for backwards-compatibility**
%PORT%	**Port number to connect to. If left like this, it will start with using the value typed in "Listen Port", but increment the port number with one, if the port is already occupied (for example by another gateway). This is repeated until there is a vacant port number. Very useful if you connect to, for example, multiple internal web sites.** **Example: Application: %BROWSER% Parameter: http://127.0.0.2:%PORT%/** **On a multiple-ports application string, the parameter is %PORTx%, where x is the number of the line, the listen port is defined in. Numbering starts from the top.**
%BROWSER%	**Full path to a local browser. If left like this, it will invoke the PC's default web browser.**
%IE%	**Full path to MS Internet Explorer on the client PC. If left like this, it will invoke Internet Explorer whether it is default browser**

	or not.
%MYPICTURES%	**Path to the logged-in user's "My Pictures" directory**
%MYDOCUMENTS%	**Path to the logged-in user's "My Documents" directory**
%PASSWORD%	**The user's password as typed in the G/On login window**
%USER_x%	**Where x is the name of a user account key. To user objects, you can add values to keys like "Mobile_Phone", "Title" or "company" The values of these keys can be parsed to the application, you are configuring.** **Refer to "Users" later in this chapter. Example: %User_Full_Name%**
%USER_auth_Domain%	**When syncing users from multiple domains in AD[EP], this parameter hold the name of the domain the user is in.**
%WINSYSDIR%	**Path to the Windows system directory, typically C:\Windows\System32**
!Registry_Key! !Registry_Key\!	**Gets its value from the Windows Registry key value of its name.** **If trailed with a backslash, it takes the value of the (default) value** **Examples:** **!HKEY_CLASSES_ROOT\Applications\iexplore.exe\shell\open** **command! = the value of the key "command" in** **HKEY_CLASSES_ROOT\Applications\iexplore.exe\shell\open** **!HKEY_CLASSES_ROOT\Applications\iexplore.exe\shell\open** **command\! = value of the (default) key in HKEY_CLASSES_ROOT\Applications\iexplore.exe\shell\open\command** **Useful i.e. for launching a registered Windows application on any language version of Windows.**
%Any Value%	**Any parameter name that has been given no value by the menu action, or from the user login will attempt to get a value from the environment on the client PC.** **Hence, if an environment value exists on the client PC, it can be**

	utilized directly from an application string. **Examples: %WINDIR% %HOMEPATH% %APPDATA% %TEMP% %PROGRAMFILES% %COMMONFILES% %TEMP%** **If the parameter name does not exist as an environment variable, it is empty/ignored when launching the application.**
%MYMUSIC%	**Path to the logged-in user's "My Music" directory**
%MYDOCUMENTS%	**Path to the logged-in user's "My Documents" directory**
%EDCSERIAL%	**Returns the unique serial number of the EDC, i.e. either the hardcoded serial number on the USB key or the serial number of host PC's harddrive. Note that on G/On installations running on VMWare machines[EP] the %EDCSERIAL% variable returns the VMWare UUID number.**

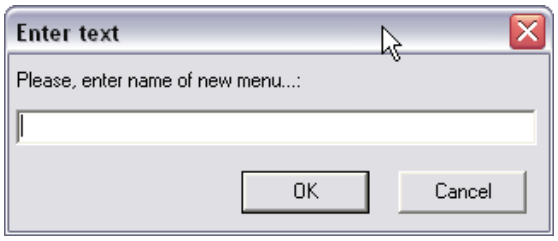
Creating Menus

The basic component of a menu is the Menu Action, so it's important to build a series of application strings and a series of Menu Actions, before you can build a menu.



To create a Menu:

1. **Go to the Menus Tab in G/On Admin**
2. **Select the [Add Menu] button**
3. **Give the menu a suitably descriptive name as this menu name will be used when the final menu is created for the user.**



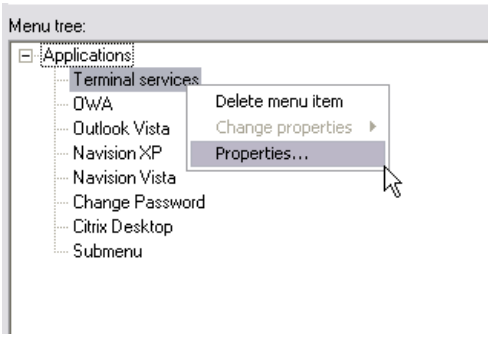
Under the list of menus, you have two tree views. The one on the left contains one item with the name of your new menu. The one on the right contains a list of Menu Actions.

The menu action list contains a couple of standard items e.g. separator and submenu, and a list of all the Menu Actions you created on the ”Menu Action” Tab.

Now create your new menu by dragging items from the right panel to the left panel, or by doubleclicking the menus in the panel on the bottom right.

Basic Features of the Menu Tab

- ❒ If you want to include something in a sub menu, then the main menu for that item or action cannot be used to launch an application (i.e. an action) – it has to be just a name for the menu. Use the Submenu action instead.



- ❒ You can delete items from the left list by right clicking on them and selecting Delete. You can't delete the root item. To do that you have to delete the whole menu.
- ❒ Placing the mouse over an item in the left tree will show you its properties.
- ❒ Doing a slow double click on an item (including the root item) lets you rename it. Highlighting and pressing F2 is another way.

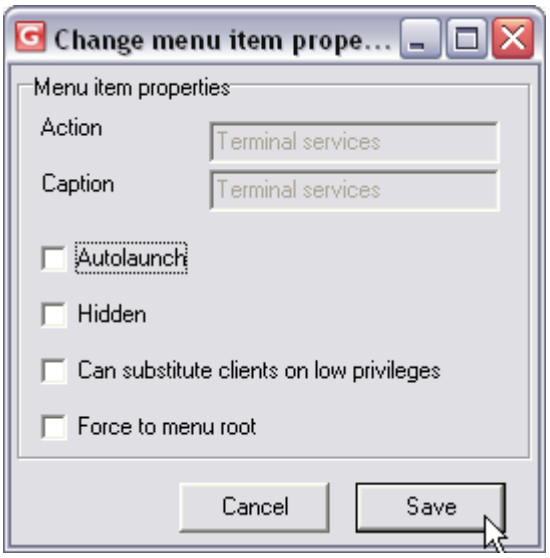
Copyright Giritech A/S 2009

- If you configure more menu items to autolaunch, the order they are executed in is top -> down in the menu tree (left pane)

> **Note:**
>
> The G/On menu already has “Exit”, “Show log” and “About” built into the root menu of any user that logs in.

Menu items properties

Right clicking on a menu item lets you change its properties. The basic properties are:



- **Autolaunch:** If this is set, the client will load this menu item upon menu load (i.e. right after login)
- **Hidden:** Don't display to the user. Use either in conjunction with the AutoLaunch property for things like gateways or if you just want to temporarily disable an item.
- **Can substitute client on low privileges:** Normally the Terminal Service client will be carried by the user on the G/On USB key. However this can give problems on "low privilege" work stations (e.g. where they are only logged on as a "guest"). This property lets the client use a TS client locally installed on the workstation.
- **Force to menu root:** To force menu items (like Exit and other frequently used applications) to the root of the users menu, check this property.

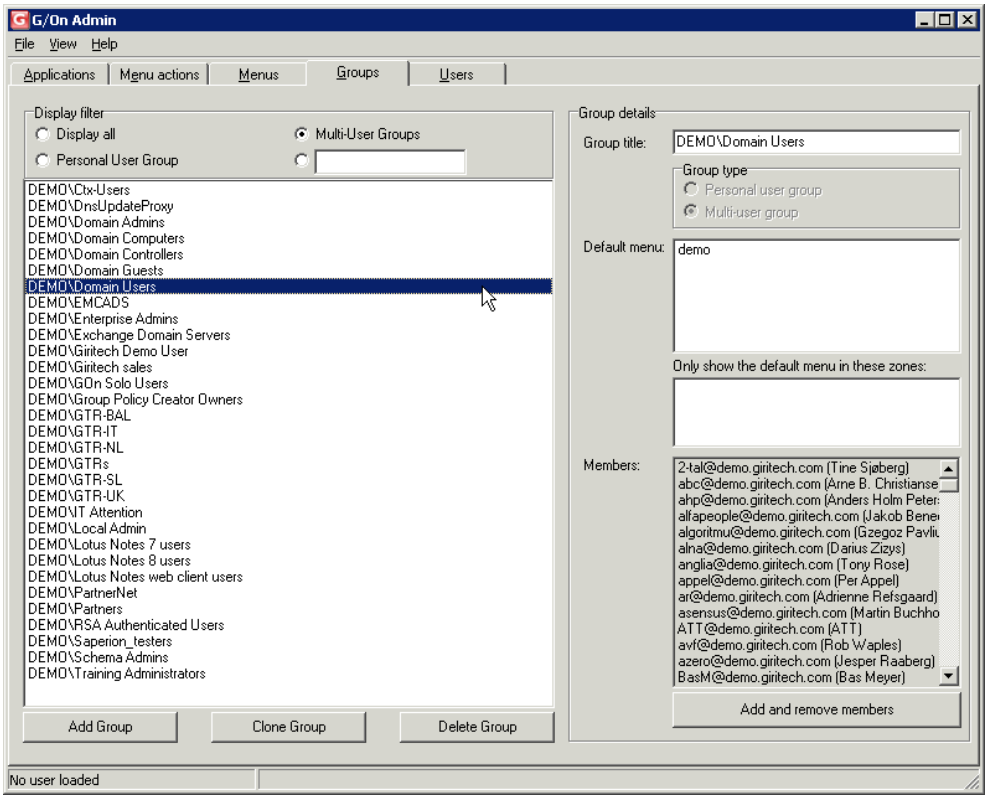
It's important to remember that the final menu presented to the user depends on group membership, and that it's possible for a user to get the contents of more than one menu. Building a practical menu structure will take some planning and a good knowledge of the company's group structure.

Copyright Giritech A/S 2009

Groups Tab

The Groups tab is reserved for managing the default Menus and assigning Zones to the User Groups you have applied to G/On.

User groups are typically managed in Active Directory and then synchronized to G/On, meaning that it isn't necessary to hand build a group structure. Nevertheless, menus need to be assigned to the user groups for the users to get a menu.



Creating Local Groups

Note:

To ensure that special groups and personal groups are NOT overwritten they must be unique names that do not exist in the AD.

AD users that are added to locally created Groups are not affected when re-synchronized with the AD. So even though the AD controls the groups and members from your domain, an AD user can be uniquely added to a Locally Created group without fear of this association being deleted when running the AD Synchronization tool.

The reverse is however not true. If you add a Locally Created User to an AD defined Group, the Local User's association will be removed the next time you run the AD Synchronization tool.

Assigning Menus

The most important thing to do is to find the relevant user groups and assign default menus. This is done by:

1. **Selecting a group from the group list on the left.**
2. **Selecting a menu in the Default menu list, by clicking on it.**
3. **Click on the menu name again to deselect it. You can only select one menu per group.**

Use the filter option to limit your view to either users (personal user groups) or multi-user groups. The default is to show only multi-user groups as these are the most used.

Creating New Groups

To create a new group right click in the group list and use either the "Add group" or "Clone group" option. "Add group" will create a new empty group. "Clone Group" will make a copy of the currently selected group, including membership.

To change the name of a group, change the title on the Group Detail frame.

Warning:

Changing a group title means the group won't sync correctly when synchronized with the AD.

Note:

Remember that group membership will be updated the next time USync or AdSync are run. And EDMS Group Memberships will not Synchronize **TO** the AD

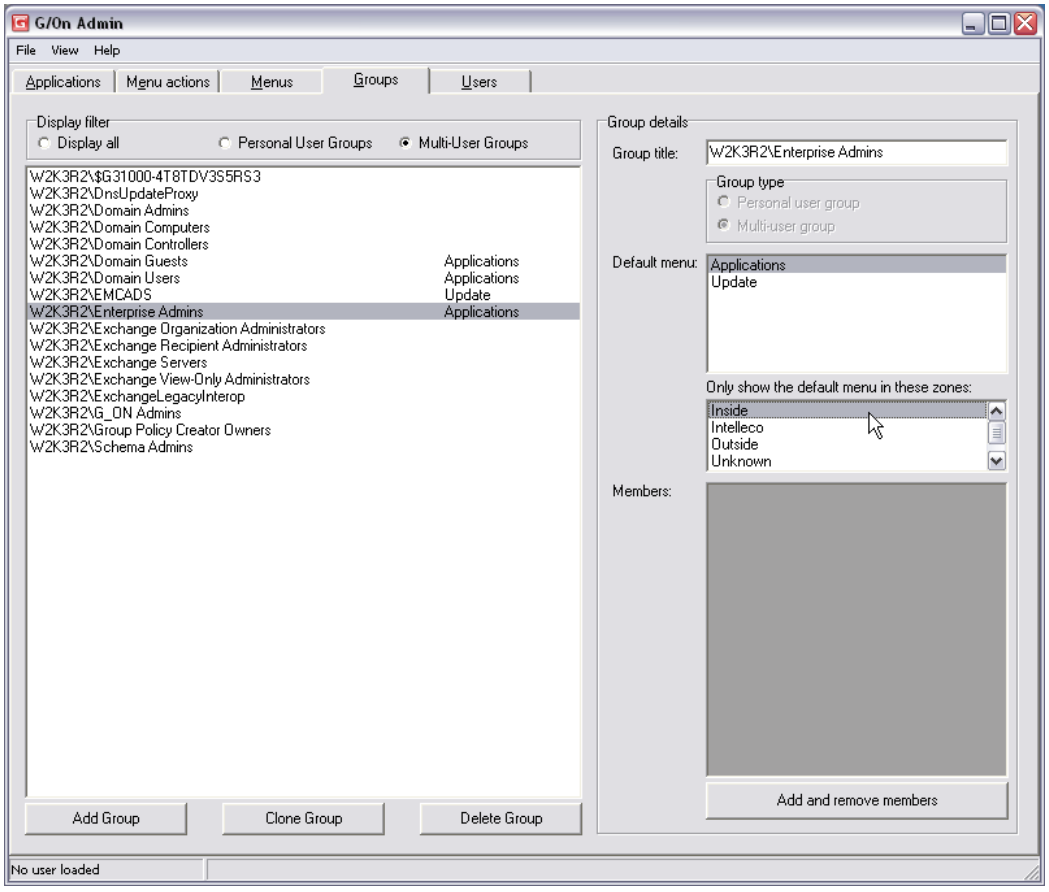
Assigning Groups to Zones

Once you have defined your Groups you will need to assign the Default Zone available to each group in each defined zone.

To complete this process you should

1. **Select the Groups Tab in G/On Admin.**
2. **Select the User Group**
3. **Verify the available Menu Items are correct**
4. **Highlight the zone or zones where this group should receive these Menus.**
5. **Repeat this process for Every Zone and Group that you have defined.**

In this example, all Enterprise Administrators, that are logging on from a client that matches the Inside Zone, will receive the menu item “Applications”



Chapter

7

User Administration

User Administration for all G/On users is centralized in the User Tab of G/On Admin.

Adding users has dependencies on whether or not syncing with AD is enabled. It is possible to have both AD synchronized users and manually added users within G/On, but special settings must be observed. Once users have been added, there are several routine management features that are included in the tool to:

Add, Edit and Delete Users

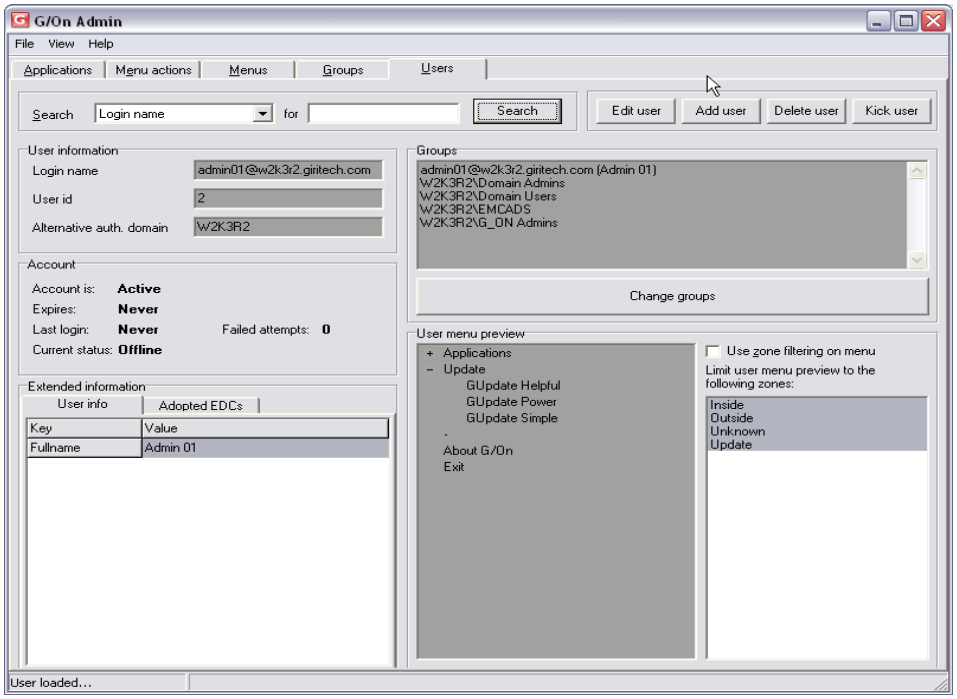
Search for Users

Checking &/or Changing Users Menus and Group Associations

Disconnect Users

Viewing Online Users

Copyright Giritech A/S 2009



Getting Started.

In G/On,you administrate Users from the G/On Admin> Users Tab.

Adding Users

Users can be added to G/On via:

- ❒ Synchronization with the Active Directory.
- ❒ Locally Adding Users

Synchronization with Active Directory

If you choose to synchronize the Active Directory you should create a G/On Specific group (default name “Emcads”) and assign the users that will be using G/On to that group.

Using the AD Synchronization tools, USync or AdSync, your users are automatically imported from your Active Directory. When syncing users from AD, only the Full_Name value is synchronized. All other values must be manually added to the User Information tab.

By default all AD Synchronized users are active (for more information on activating users see section Activating/Enabling Users later in this chapter)

Warning:

Changes made in G/On to AD defined Groups and users will be overwritten the next time you synchronize with the AD.

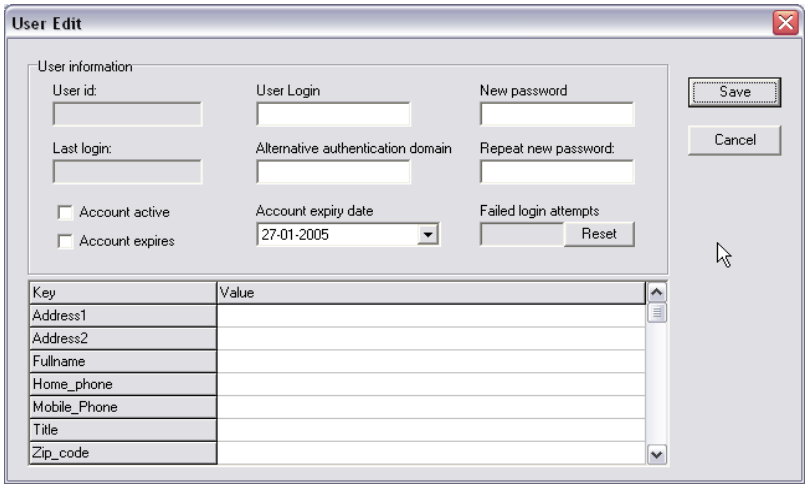
Management of groups, their associated menus and zones are explained in Chapter 6.

Locally Adding Users

You have the possibility to create users directly in G/On.

To Add a User:

1. **Go to G/On Admin >Users Tab > Add User**
2. **In the User Edit Window, enter the credentials of the user**
3. **Activate the Account by checking "Account active"**
4. **Save the user by pressing "Save"**



Note:

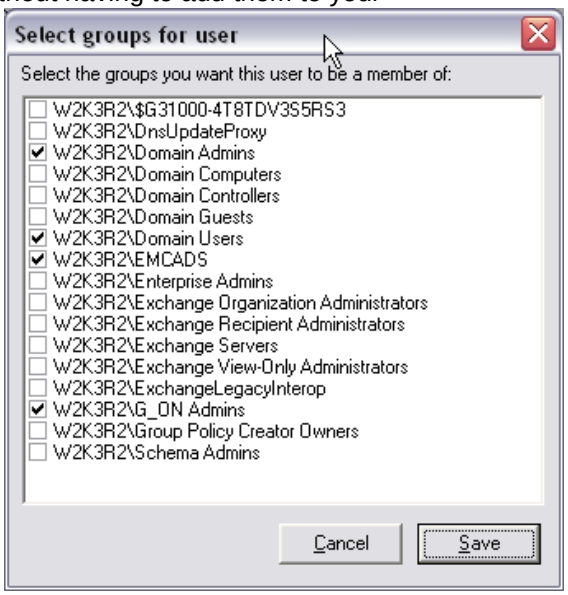
Manually added users are not automatically activated. You have to check the box "Account Active" before the user can log in.

Using both AD and Local Users

There are many reasons to employ a mixed user policy in G/On. In many companies, you have external vendors, temporary employees or partners that you don't want added to your corporate network or AD. G/On enables you to locally create users and define restricted access without having to add them to your domain or your AD.

Assigning/Changing a Users Group Association:

Instead of using the group page to add and remove users to a group, you can add and remove a user from several groups on the user page by using the **Change Groups** button. This will show a dialog box containing all (multi-user) groups and an option to add or remove check marks to indicate membership.



Note:

To ensure that special groups and personal groups are NOT overwritten they must be unique names that do not exist in the AD.

For example you have a vendor/supplier that you would like to provide ERP services to. You would create a personal user group for this user in G/OnAdmin that might be called “VendorName”. This user and group is in not in the AD so when the EDMS is synchronized, the user will remain intact.

Warning:

AD vs. Local Users and Group Association:

AD users that are added to locally created Groups are not affected when re-synchronized with the AD. So even though the AD controls the groups and members from your domain, an AD user can be uniquely added to a Locally Created group without fear of this association being deleted when running one of the AD Synchronization tools.

The reverse is however *not* true. If you add a Locally Created User to an AD-defined Group, the Local User’s association will be removed the next time you run one of the AD Synchronization tools.

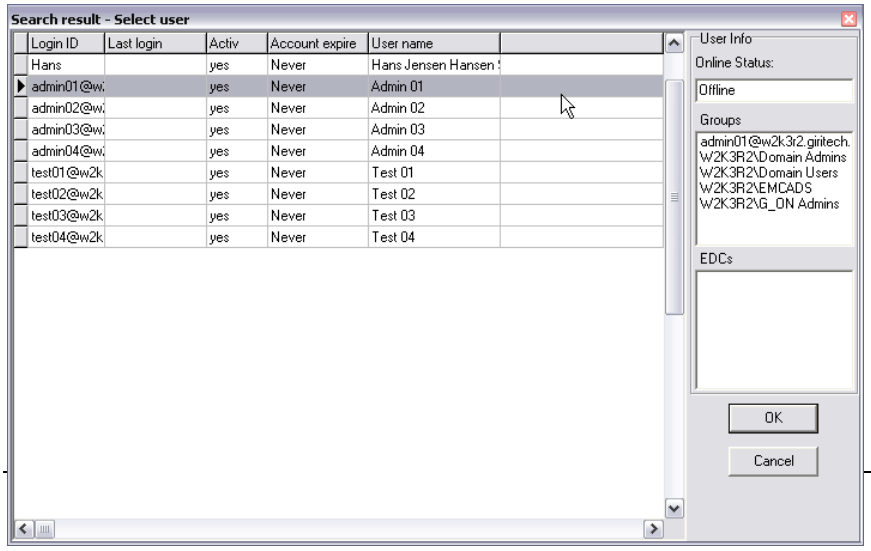
Checking that a user gets the right menu

In the lower right corner of the user page you can see a preview of how the user's menu will look when logging in.

Selecting/Searching Users

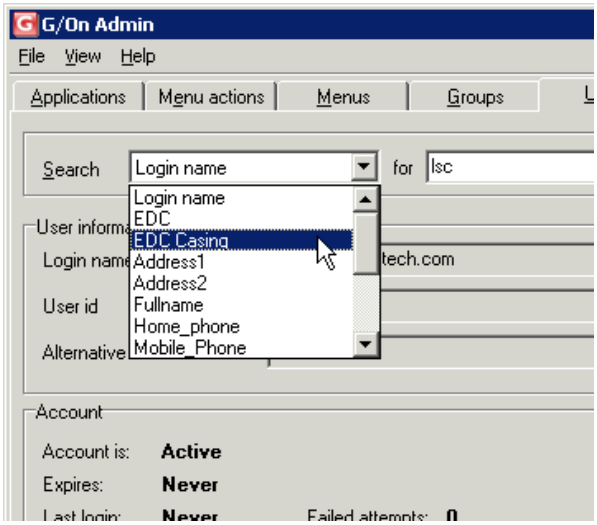
To select a User:

1. **Go to the User Tab> Search User**
2. **Select the User from the List in the Search Result Window and double click.**
3. **The selected user’s details will now appear in the User Tab.**



Note: It is possible to search using other parameters than login name (e.g. Address fields, Title or EDC serial number). This is done by selecting another property from the search dropdown box.

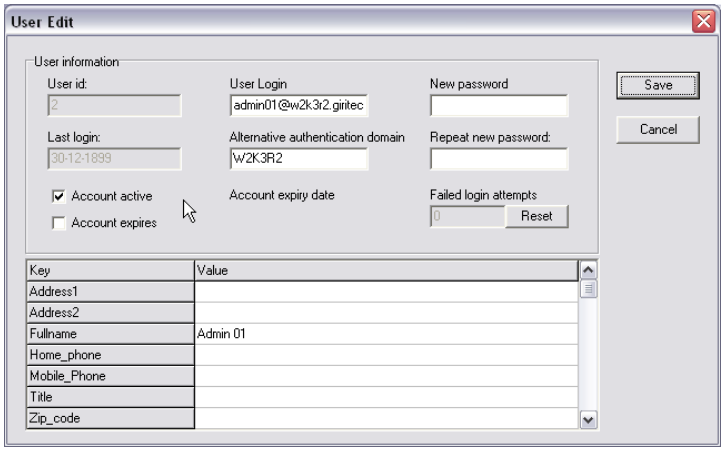
The searched field will then be included in the search result dialog.



Activating/ Enabling Users

Users synchronized from the Active Directory are enabled by default and no extra actions are necessary.

Locally created users must be manually enabled by checking the account active check box.



Enabling Locked Out Users

In G/On Builder you defined the number of failed attempts each user is allowed before being locked out of the system. If a user is locked out, the account is de-activated. To reactivate their account you must:

1. **Go to G/On Admin > User Tab > Edit User**
2. **Check the Account Active**
3. **Evaluate if you want to reset the number of failed login attempts**
4. **Save Changes**

Deleting Users

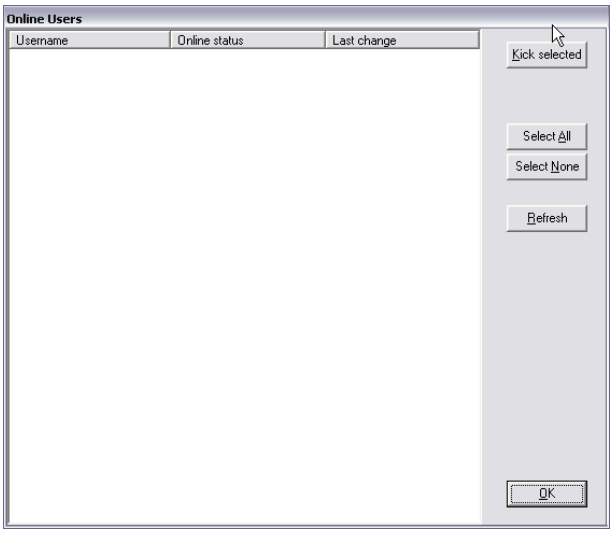
To Delete a User

1. **Go to G/On Admin > User Tab > Delete User**

> **Note:**
>
> Only Locally Created users are permanently deleted with this function. If you delete a user that has been defined by your Active Directory, The user will be added the next time you synchronize unless you remove the G/On association from the User in the Active Directory

Viewing Online Users

2. **Go to G/On Admin > File > Online Users**



Disconnecting Users

1. **Go to G/On Admin > File > Online Users**
2. **Highlight the user you want to Disconnect**
3. **Click "Kick Selected"**

Alternately, you can disconnect a user directly from the User Tab by selecting the button > **Kick User.**

> **Note:**
>
> Permanent removal of the adopted EDC is the only way to deny a user future access to the G/On system. If you don't remove the user's EDC from the adopted EDC list before disconnecting them from the system, the user can still re-connect to the G/On server.

Chapter 8

Adopting Users

One of the key elements protecting anyone from accessing your system via G/On is User Adoption. While Zones and Group Rules/Menus can determine what is seen, the adoption process ensures that only the users you know and have authorized can attempt to access your G/On Installation.

Now you have completed your G/On Admin Configuration, it's time to decide which method to use to adopt your users. In this section you will learn about adoption, the elements of identification with the EMCADS™ Data Carrier (EDC) and importance of your G/On Identity file.

You will be using 3 primary interfaces in G/On Admin and Access rules manager to:

Import EDCs

Adopt Users and Clients

Manage Adopted Users and EDCs

Users can be adopted in three ways:

1. Adopt from File
2. Adopt by Request
3. Auto-Adoption[EP]

Note:

One of the user keys delivered from Giritech manufacturing is specially marked, containing the file EDCSERIALS.DAT. This should be copied to the G/On Server after you have completed the server installation and before you deploy user keys.

What is being Adopted

In the adoption process, you are adopting the EMCADS™ Data Carrier (EDC) serial number.

The EDC serial number is contained within the G/On Client Identity Facility (CIF). The EDC serial number is either the unique serial number burned on the G/On USB key, or the unique identifier of the PC device where G/On Desktop is installed.

Warning:

G/On release 3.6 uses a new EDC detection routine for identifying the computers from which access is given. This means that *all* desktop clients adopted with G/On version 3.5 or older will have to be re-adopted after installation of G/On 3.6. **See also section:** Notes on G/On Desktop Adoption **on page 106**

Why Adoption is Important

By adopting the EDC into your system, you maintain control over who is accessing your Server.

The EDC, CIF and Identity File are important elements to your G/On System, without them your clients can't connect or gain access to the system.

- ❒ The Identity File gives clients the ability to connect to the G/On Server
- ❒ The EDC is your Client Specific Unique Serial Number

Identity File

When the G/On Server is installed and configured, a unique file, named the identity file, is created. This file contains information unique to the G/On installation, and the identity file is what gives the G/On USB and G/On Desktop clients the ability to connect to the G/On Server. The identity file is encrypted during creation, and can safely be distributed to the clients by electronic means.

The initial connection happens when the G/On USB or G/On Desktop clients is first launched. The client decrypts the identity file to get the IP name/address of the G/On Server to contact. The client contacts the server, the server responds with a greeting, and the secure key exchange (SKE) process starts.

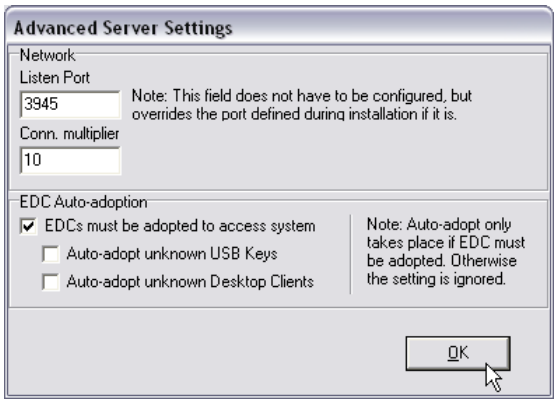
Secure Key Exchange (SKE)

A greeting with a per-session public ECC key and a signature is sent from the server. Only a client with an identity file created by this specific server can validate the signature of the public key. This is the basis for the mutual authentication, ensuring the server and client is configured for each other. The client responds to the challenge with the client identity facility (CIF).

If the client is unable to present the correct response, the TCP connection is terminated immediately. This is also the response to connection attempt from anything that isn't a proper client, i.e. telnet to port 3945/tcp on the G/On server.

Copyright Giritech A/S 2009

G/On Builder Settings for Adoption


Advanced Server Settings
Network
Listen Port
3945
Note: This field does not have to be configured, but overrides the port defined during installation if it is.
Conn. multiplier
10
EDC Auto-adoption
EDCs must be adopted to access system
Auto-adopt unknown USB Keys
Auto-adopt unknown Desktop Clients
Note: Auto-adopt only takes place if EDC must be adopted. Otherwise the setting is ignored.
OK

In the Advanced Server Settings for EDC Auto-adoption[EP], the checkbox for "*EDCs must be adopted to access system*" must be selected in order to utilize the adoption features in G/On.

If you selected the Auto-Adopt[EP] unknown features for either USB keys or Desktop you do not have to manually adopt or import EDCs from the file.

The Auto-Adopt Feature[EP] means that any EDCs that have your company's identity file will be able to access your system. They will automatically match into the zones you have defined and no further action is necessary.

If you chose the Auto-Adopt feature[EP], you can still choose to manage the EDCs by assigning or locking them.

Warning:

Auto-adopt features[EP] should be used with caution because improper use of Auto-adopt circumvents security best practices as this feature enables anyone that receives your identity file to connect to your company.

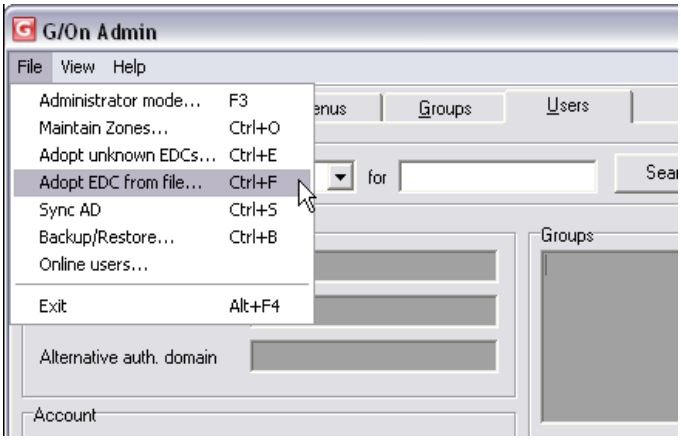
Adoption of EDCs is one of the security best practices that can be aligned with your security policy. If you need guidance on how to align Adoption with your security policy, please contact support@giritech.com

Adopt EDC from File

When you receive your G/On Product, one of the user keys has been specially marked. It contains the file EDCSERIALS.DAT.

To import your EDCs and adopt them from the file:

1. **Go to G/On Admin**
2. **Select File > Adopt EDC from file**
3. **Browse to the EDCSERIALS.DAT file > OK.**
4. **You can now proceed to the section on Assigning/Locking EDCs or proceed directly to Client Deployment.**

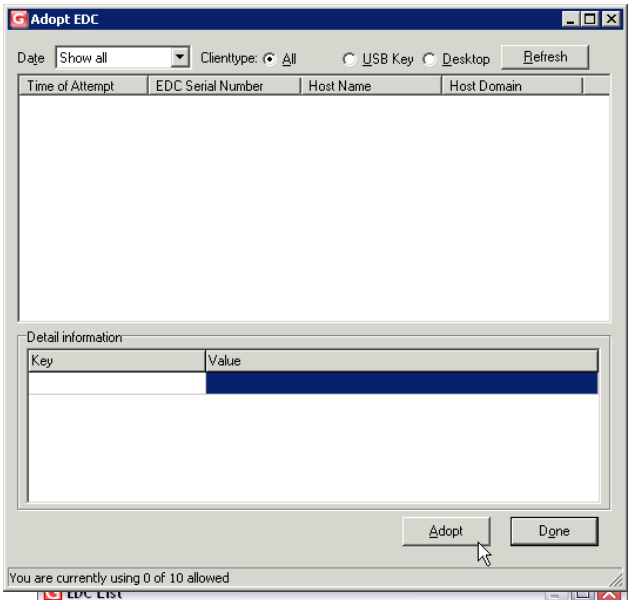


Manually Adopting EDCs

You can manually adopt EDCs from either the

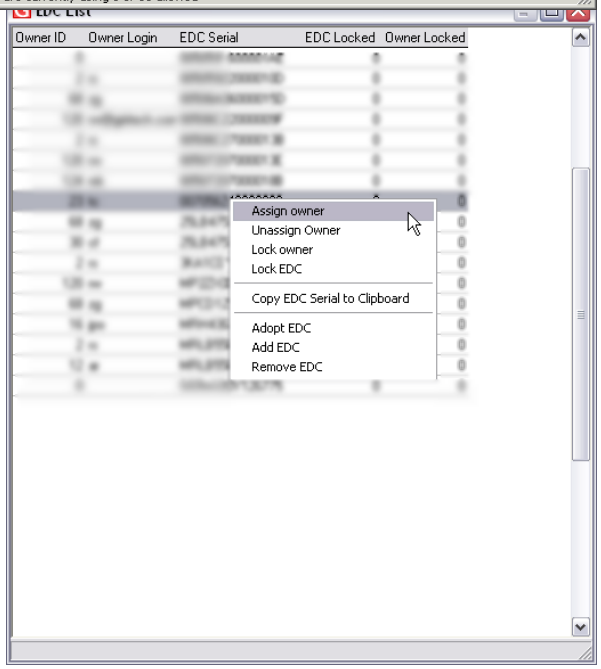
Access Rules Manager by right clicking anywhere on the EDC Rules Admin Window and selecting Adopt EDC

G/On Admin Tool. by selecting File > Adopt Unknown EDC



Assigning/Locking EDCs

1. **Log into the Access Rules Manager**
2. **Right click anywhere on the EDC Rules Admin Window and select "Show EDC List"**
3. **In the EDC List Window select the on the EDC you would like to assign > right click**
4. **Select the appropriate action from the list:**



Assign Owner: assigns EDCs to users. Officially assigns responsibility of the EDC to a named user.

Lock Owner: If you lock the owner, then the user can only use this EDC and no other EDC. However many users can still be configured to use the same EDC!

Lock EDC: This EDC can only be used by this person thus disabling any other user from using this specific EDC.

Edit Casing Serial: this entry allows you to enter the external serial number that is laser engraved on the USB keys and associate it with the internal unique ID of the key that only the G/On system can read. This eases administration of lost key's as they can be associated with user profiles using the external ID on the key without jeopardizing the security of the internal serial ID.

Adopt/Add/Remove EDCs. Adopt new EDCs that has tried to contact the G/On Server or manually adding new EDCs. Removing EDCs that needs to be locked-out from the G/On server.

Copyright Giritech A/S 2009

Chapter

9

Distributing & Deploying Clients

Client distribution and deployment is one of the most critical steps in your G/On installation. Proper distribution, EDC adoption and deployment involve aligning the physical distribution methods with your internal security policies.

Once you have completed your G/On Configuration, it's time to decide how to adopt , distribute and deploy your clients to the users. The Best Practice Distribution methods found in this chapter can help you determine which method best aligns with your security best practices. Once you have decided which client distribution method to use it is time to deploy the clients. In this section, we introduce you to the basic concepts for our update and deployment tool G/Update.

Client Deployment :

Choose which client distribution method meets your Security Guidelines

Align the EDC adoption process with your client distribution best practice

Verify your installation is configured to use the update and deployment tool

Note:

One of the user keys is specially marked, containing the file EDCSERIALS.DAT. This should be copied to the G/On Server after you have completed the server installation before you deploy user keys.

Best Practice Distribution Methods

There are two things you have to distribute to G/On users.

- ❒ Identity File
- ❒ USB Key and/or the Desktop Client

How the "Identity" file is distributed, depends on the level of security enforced by your security policy.

USB Key and Identity File

For maximum security, Administrators should copy the “Identity” file directly from the G/On Server to the G/On USB Key, before hand-to-hand distribution of the G/On USB Key to the user.

Another approach would be to place the “Identity” file on the intranet, and allow the user to copy the file from the intranet to the Read/Write partition of the G/On USB Key. The most secure option in this scenario would require the user to deploy the G/On USB Key while connected to the intranet.

The approach for external users will differ, if it is not possible for them to physically present themselves at your location. The most secure option would be to send the G/On USB Key as registered mail, and forward the “Identity” file as a zipped file, in an e-mail.

There are risks, with remote deployment, which could potentially expose your identity to unwanted parties. However, for ease of deployment, this may be a practical course of action, and since G/On employs 2-factor authentication, a username and password is still needed, along with the adopted EDC of the G/On USB Key.

Desktop Client and Identity File

The desktop client is found in the EMCADS folder, typically C:\Program Files\Emcads\GOnDesktop. This file contains both the Installer and your identity file.

The desktop client can be mailed to users with or without the identity file. Or the Desktop Client can be pre installed as part of a corporate image. You should align the method for distribution with your own best practice security guidelines.

PLEASE SEE Notes on G/On Desktop Adoption on Page 106 before deploying G/On Desktop Clients.

Distribution Methods Step by Step

Pre-Adopting USB Key Clients

Pre-Adopting clients can be used to speed the adoption process for G/On USB Key deployment. The best way to pre-adopt clients is to

1. **Import and Adopt the EDCs from the EDCSERIALS.DAT file on the specially marked USB key.**
2. **Manage the EDCs by Assigning or locking it to the user**
3. **Distributing the Keys or Clients / Identity files by requiring the users to sign a receipt**

Copyright Giritech A/S 2009

Adopting Clients after connection

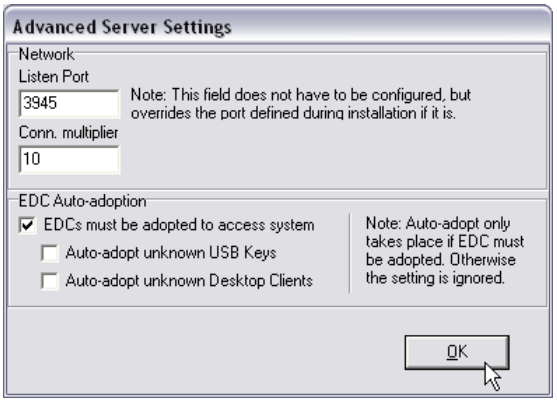
Adopting Clients after they have tried to connect can be used with either G/On USB Keys or G/On Desktop Clients.

In this scenario, the user will try to use the key to connect. But they will receive a message that their attempt has been denied and logged. Once this has occurred you should ask:

1. **The users to contact the G/On Administrator and let them know they have tried to connect**
2. **The Administrator can use Access Rules Manager by right clicking anywhere on the EDC Rules Admin Window and selecting Adopt EDC or use the G/On Admin Tool by selecting File > Adopt Unknown EDC**
3. **The Administrator can then choose to just adopt the EDC or they can further decide to adopt and assign or lock it to the user.**

AutoAdopting Clients[EP]

If you have selected either of the autoadopt features[EP] in G/On Builder> Advanced Server Settings, then anyone with your identity file will be automatically connected to your system.


Advanced Server Settings
Network
Listen Port
3945
Note: This field does not have to be configured, but overrides the port defined during installation if it is.
Conn. multiplier
10
EDC Auto-adoption
EDCs must be adopted to access system
Auto-adopt unknown USB Keys
Auto-adopt unknown Desktop Clients
Note: Auto-adopt only takes place if EDC must be adopted. Otherwise the setting is ignored.
OK

Note: We do not recommend that you use the Auto-adoption feature[EP] with USB Keys. We also advise using extreme caution when applying to desktop clients.

- **To manage Auto-Adopted[EP] Clients, the Administrator should routinely go into the EDC List to assign owners, lock EDCs or Lock Owners.**

Security Warning:

Auto-adopt features[EP] should be used with caution because improper use of Auto-adopt[EP] circumvents security best practices as this feature enables anyone that receives your identity file to connect to your company.

Adoption of EDCs is one of the security best practices that can be aligned with your security policy. If you need guidance on how to align Adoption with your security policy, please contact support@giritech.com

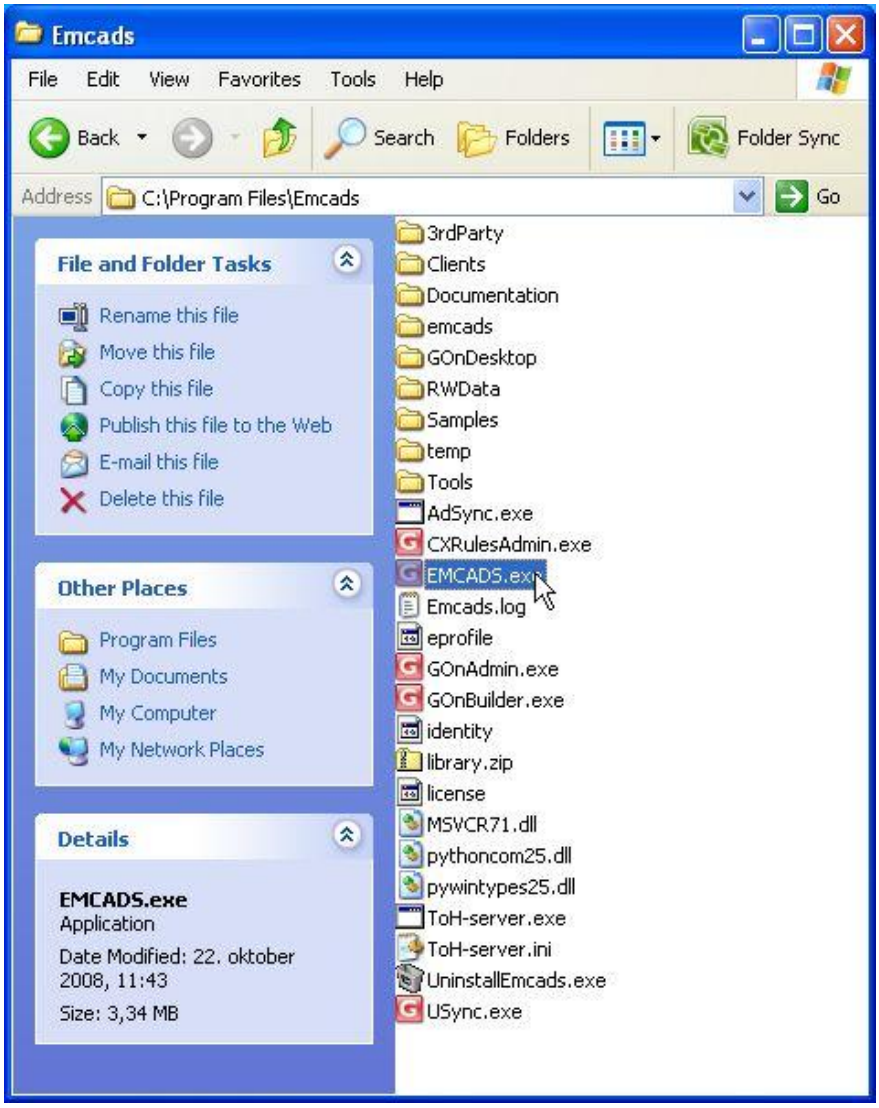
Deploying Clients with G/Update

Once you have decided which client distribution method to use it is time to deploy the clients. In this section, we introduce you to the basic concepts for our update and deployment tool G/Update.

G/Update is the update and deployment toolkit from Giritech. It is designed to ease the deployment of the G/On client software, as well as pushing out updates when necessary.

The EMCADS install directory on the G/On Server contains two folders named “Clients” and “RWData”. These folders contain the G/On client software and the software that goes on to the Read/Write partition respectively.

> **Note:**
>
> The content from the Client folder goes to the Read/Only Partition of the key, while the RW Data goes to the Read/Write partition.



Deploying G/On USB Clients

The G/On USB Key has been initialized before shipping from Giritech. The G/On USB Key contains G/Update, necessary for deploying the key, with the proper software, from the central G/On Server.

Note:

To run G/Update, the G/On Client EDC must either be already adopted on the G/On Server, or the "Auto Adopt" feature[EP] must be turned on. Consult Chapter 8 on Adoption for more information.

1. **Copy your Identity file from C:\Program Files\Emcads\Clients to the USB Key.**
2. **Distribute the Keys to the Users**
3. **Instruct the Users to Insert the Key and follow the Instructions.**
4. **Depending on which Adoption process you have employed, you may be required to Adopt or manage the USB Keys after the user attempts to connect but before G/Update can complete the deployment of the key.**

Warning:

When the key is in the process of deployment, users should NOT remove the G/On USB Key from the computer during the update as this could permanently damage the device.

Users should also monitor their power. If the host machine loses power during this critical phase of the update process then the G/On USB Key will very likely be permanently damaged.

Finally, during the ISO recording process (the "burning" of data onto the USB key's Read/Only partition), the G/Update software will NOT respond to user input, it will switch to stay "on top" of other applications and will not redraw.

After the recording is completed, all files copied off the Read/Write partition will be copied back.

The user can click the "Show Log" link in the lower right corner of the G/Update user interface to see a more detailed log of the progress.

Deploying Desktop Clients

1. **Copy the Installer and Identity files from C:\Program Files\Emcads\GOnDesktop**

   TIP: If you are placing the G/On Desktop Client on a corporate image, you can omit the identity file. When later authorizing a user to remotely access your system you can provide them with the identity file and

proceed with your normal adoption process.

3. **Distribute the Desktop Client/identity file to the Users**
4. **Instruct the Users to double click on the G/On Desktop Installer to initialize the installation and connection process.**
5. **Depending on which Adoption process you have employed, you may be required to Adopt or manage the Desktop clients after the user attempts to connect but before G/Update can complete the deployment.**

Note:

To run G/Update, the G/On Desktop Client EDC must either be already adopted on the G/On Server, or the "Auto Adopt" feature[EP] must be turned on. Consult Chapter 8 on Adoption for more information.

Please be aware that the described default installation only installs the basic G/On clients delivered with G/On on the desktop. If you need to include any special clientside software you will need to direct the user (or force the user via a menu item) to run a G/On Update with parameters ***/getall*** and ***/updaterw*** (please refer to the section on G/Update for more details on additional parameters).

Warning:

G/On release 3.6 uses a new EDC detection routine for identifying the computers from which access is given. This means that *all* desktop clients adopted with G/On version 3.5 or older will have to be re-adopted after installation of G/On 3.6.

Distributing Identity Files

If the Desktop client is installed as part of a corporate image without the IDENTITY file, in order to fully deploy the G/On Desktop client you will have to distribute or post the IDENTITY file on a network share. Instruct the user to copy the IDENTITY file to C:\Program Files\ GOn Desktop\ and Launch G/On.

If you have chosen the "Manual Adoption Method" the user will have to contact the System Administrator to be adopted. Here the Administrator can review the user's PC information and ask the user questions about these PC details before granting access.

Instructing Users to Deploy Keys

1. Insert your new G/On USB Key into a PC running any of the operating systems supported. Give the PC time to recognize the new hardware device.
2. If the Key is Adopted, the user will receive a message asking if they would like to deploy the key. Click "Yes"
3. When the update is complete, close the G/On Update Manager by clicking on the red "X" in the upper-right corner.

Note:

The update process can be lengthy and it may seem that the update process stops, but it can take several minutes. It is important the update

process be allowed to complete, otherwise the key is left in an unknown state, and may require a new initialization.

The G/On USB Key is now ready for use. Remove the G/On USB Key and reinsert it to connect to the G/On Server.

Setting up Zones for New Key Deployment

Not necessary for initial client distribution and deployment

Setting up Application Strings for New Key Deployment

Not necessary for initial client distribution and deployment

Notes on G/On Desktop Adoption

G/On 3.6 introduces a new method for determining the unique hardware identification of the PC device. This identification, the EDC, is used as the hardware part of the two-factor authentication in G/On. The new method is using the MAC address of all enabled network adapters together with Windows license information. Subsequent identification of adopted devices will be satisfied if just one on the network adapters and the Windows license are recognized.

Deploying and Adopting G/On Desktop:

1. Ask the user to install G/On Desktop and ask them to make first connection attempt either via the G/On Desktop Menu in the Windows Program Menu or by running EClient.exe or GUpdate.exe.
    - At this time the G/On Desktop client will generate the unique identification that requires adoption in the G/On Server
2. Adopt the G/On Desktop client either in G/On Admin or in CxRulesAdmin.
3. The G/On Desktop Client is now ready for use.
   After adoption, the G/On Desktop client will be recognized and allowed access as long as one of the adopted network adapters is enabled.

NOTE: Some users may in rare occasions disable the network adapter that was used in the adoption process. Typically, the cable network adapter is always enabled and will always be included in the adoption process. If a user for some reason subsequently disables the cable network adapter, the G/On server will reject the connection attempt. In such case, simply instruct users to enable their network adapters.

G/On Desktop Users Upgrading from G/On 3.5 or previous version.

The new method for determining the unique hardware identification of the PC device in G/On 3.6 means that all existing G/On Desktop clients must be re-adopted. Existing G/On Desktop EDC's can be deleted in the tool CxRulesAdmin or in GOnAdmin.

Chapter 10

Upgrading Clients

When making changes to your existing G/On solution or after you upgrade to another version of G/On, you will need to upgrade your already deployed clients.

There are several reasons for updating an adopted G/On USB Key, besides upgrades of the client software. If any of the G/On Server's security settings are changed, or a new signing key pair needs to be created, the G/On USB Key must be updated.

Warning:

G/On release 3.6 uses a new EDC detection routine for identifying the computers from which access is given. This means that *all* desktop clients adopted with G/On version 3.5 or older will have to be re-adopted after installation of G/On 3.6. **See also section:** Notes on G/On Desktop Adoption **on page 106**

How G/Update works on Upgrades

When G/Update runs normally - either invoked manually by the user directly or forced to run by creating an update zone, the client will connect to the G/On server that it belongs to and look for updates (or changes) to the files on the Read/Only partition of the G/On USB Key or the Desktop client directory**.**

If G/Update finds anything to update, it will download the needed files from the server, and, just before the actual update is performed, shut down the G/On client, if it is running. If there are no updates, the G/On client is left running as it were.

Note:

G/Update updates the Read/Only partition from the .\Clients folder under the EMCADS installation folder. There is one limitation - it does NOT download ISO image files from the root of the .\Clients folder, which is where pre-recorded ISO images for deployment are stored.

If updates are available, G/Update will notify the user by displaying a dialog box asking if the user wants to download the updates.

Copyright Giritech A/S 2009

The user can determine if the bandwidth is sufficient for the download and abort it if the client software is used over a slow connection, like GSM or a low bandwidth connection.

If the user selects to continue, G/Update will continue to download and prepare the updates. G/Update will show which file it is currently downloading.

When the download is complete, G/Update will prepare the new ISO image for the Read/Only partition of the G/On USB Key. This includes importing all files from the Read/Only partition that were not updated.

The last step before recording the data onto the Read/Only partition is to offer a safety backup of all the data on the Read/Write partition. This is done because any data in the Read/Write partition will (in most cases) be deleted as the G/On USB Key is re-partitioned to accommodate the new ISO image.

Typically, the user will answer “Yes” to this question.

Automating update of the Clients and the Applications after upgrade

The easiest choice for users is to automate the update procedure. You can choose to automate the update procedure by:

1. **Creating an update zone**
2. **Creating G/Update Application String Simple Template**
3. **Creating 2 G/Update Menu Action Items from the Simple G/Update Template**
    a. **One for forced update of the R/O partition**
    b. **One for manual update of the R/W partition**
4. **Creating 2 Update Menu Items**
    a. **One for the update of the R/O partition with properties set to hidden & auto-launch**
    b. **One for manual update of the R/W partition that is on the users menu**
5. **Assigning the Menu Item to the User Group(s)**
6. **Assigning the User Group to the Zone**

Note:

Automation will only update the Read/Only partition of the USB Key.

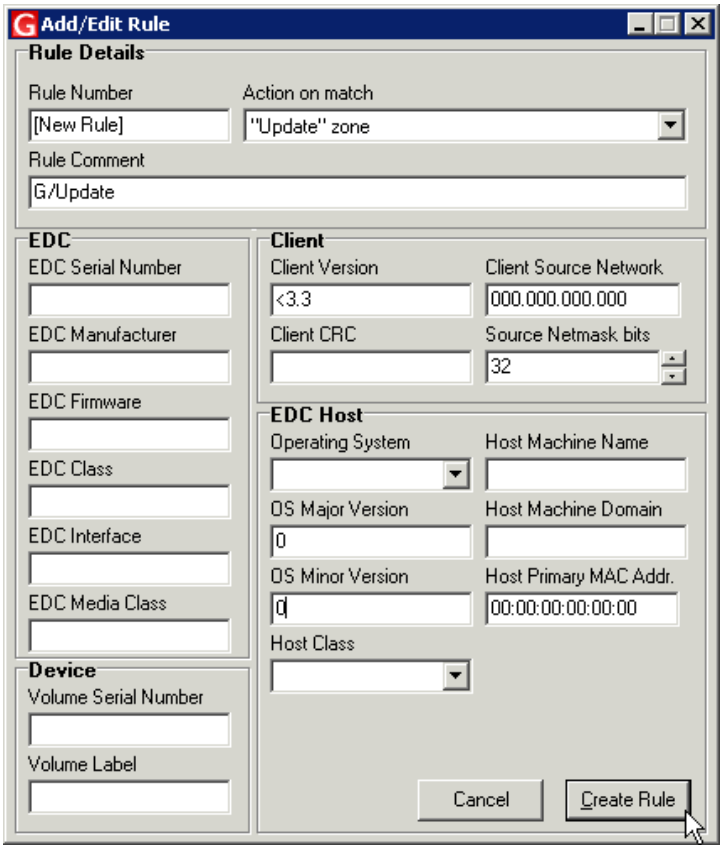
To update the Read/Write Partition you will have to ask the Users to manually select the Update RW Menu Action (described Below)

Upgrade Warning:

It’s important to instruct users to update the Read/Write partition of their G/On client after you have upgraded from a version older than 3.3. This is to capture the changes to the new RDP 6.0 that is included from release 3.3 and onwards. RDP, GRDP or the 3.4/.5/.6 GTSC clients may not launch if the Read/Write partition is not updated.

Automatically Update Clients Read/Only Partition

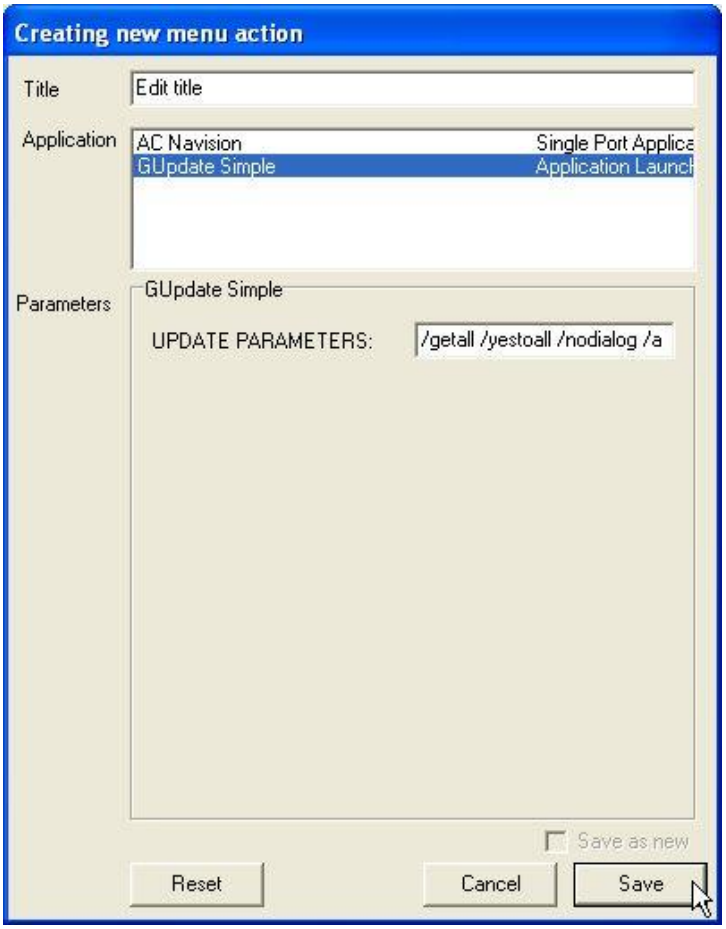
1. **In the Access Rules Manager, you can create a new zone for updates. Note that you will have to stipulate which Client version you are upgrading to. In this example we are going to force an upgrade of the Read/Only partition on any client less than 3.3**



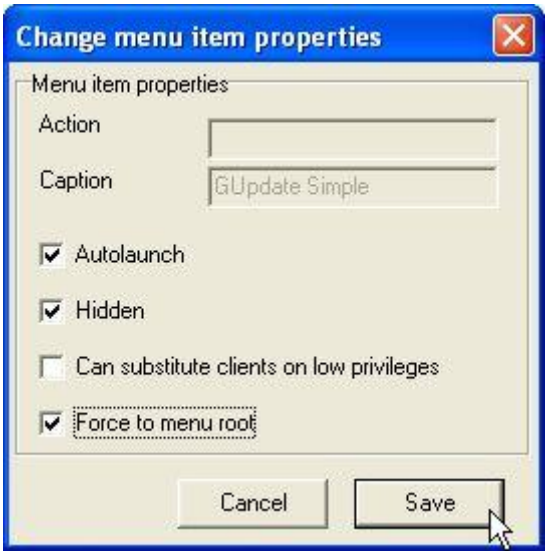
2. **Next you need to create an application string to update the clients and the applications. In G/On Admin go to the Applications Tab and choose the Application Creator button. Next choose the GUpdate button from the Application Creation Wizard.**

3. **You can choose from any of the string types, we have illustrated the G/Update Simple in this exercise.**

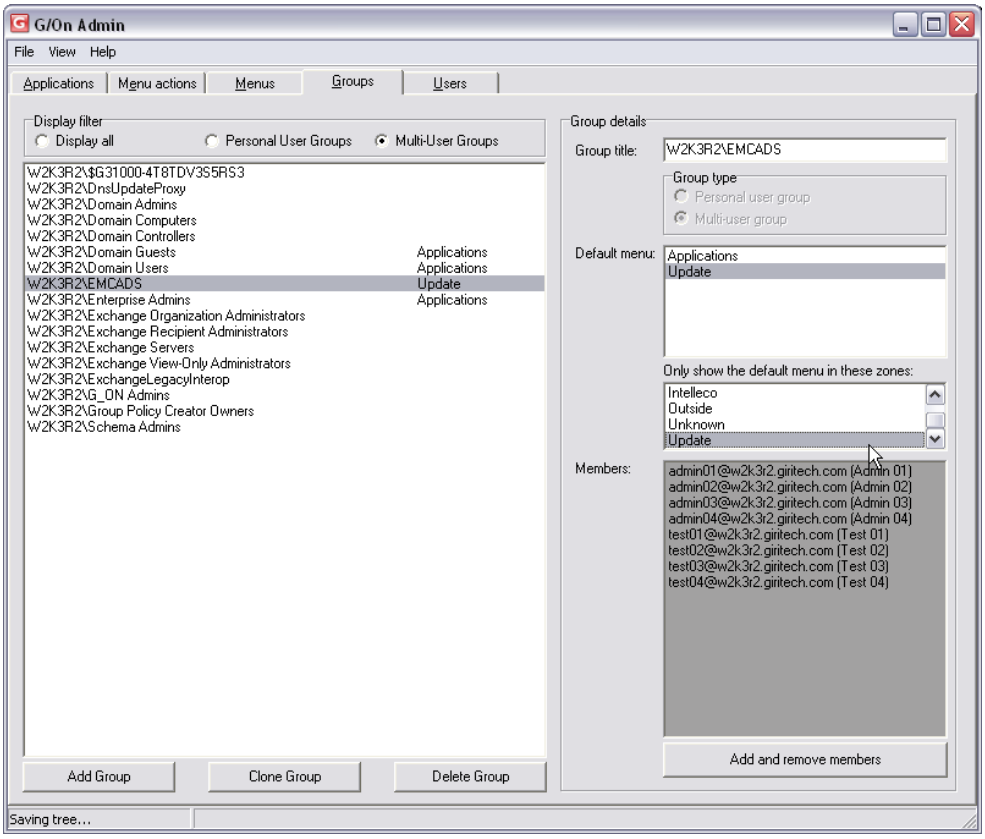
4. **Go to the Menu Actions tab and select > Create New Action**
5. **Select the GUpdate Simple Template**
6. **Name the Title of the Menu Action "Update G/On RO Partition"**
7. **Fill in the parameters: /getall /yestoall /nodialog /autoclose /launchgon and press Save**



8. **Go to the G/On Admin > Menus Tab > select Add Menu > Enter the name "G/On Update CD Menu" and assign the "Update G/On RO Partition" menu action to this by double clicking on it.**
9. **Right click the "Update G/On CD Menu" and select Properties. Check the "Autolaunch", "Hidden" and "Force to menu root" buttons >SAVE**



10. **Then in the Groups Tab. Apply the Menu Items to the Update Zone. This will automatically update the clients that match the update zone.**



Copyright Giritech A/S 2009

Manually Update Clients Read/Write Partition

1. **Go to the Menu Actions tab and select > Create New Action**
2. **Select the GUpdate Simple Template**
3. **Name the Menu Action "Update G/On RW Partition"**
4. **Enter the parameters: /getall /yestoall /nodialog /updaterw /autoclose /launchgon**
5. **Go to the G/On Admin > Menu > Select the Update Menu > Drag assign the "Update G/On RW Partition" menu action to this.**
6. **Right click the "Update CD Menu" and select Properties. Check Force to Root >SAVE**
7. **Notify Users via Email to Select the menu item to update their Read/Write partition.**

Creating an Update Menu Item:

If you don't want to automate the entire procedure, You can choose to manually inform the users, for example via email, to run their G/Update. The steps to configure the Update Templates for the Read/Only and the Read/Write partition are basically the same but you do not need to create an Update Zone or use the Menu parameters to hide, autolaunch and nodialogue,

Instructing Users to Manually Update their Clients

Desktop Clients

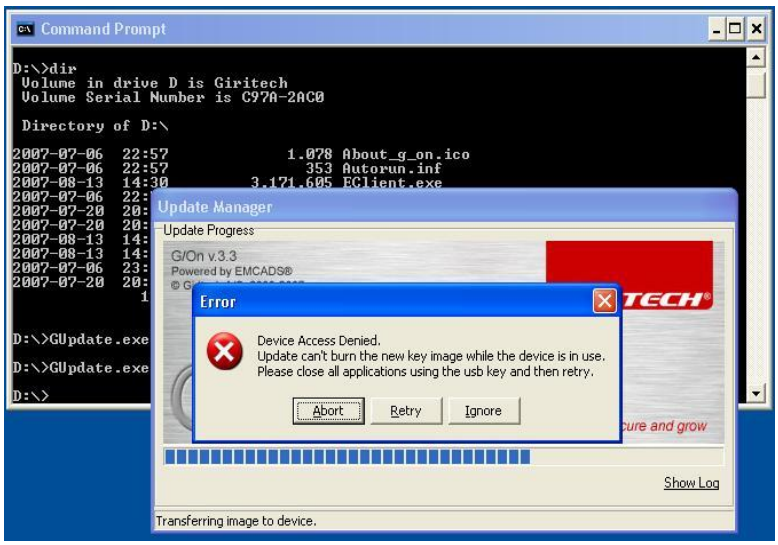
For Desktop Clients the user should be directed to launch **G/Update** from the directory where the Desktop client was installed, usually *C:\Program Files\GOn Desktop*.

Please refer to the note on page 41.

G/On USB Key

Users should be instructed to go to "My Computer" and select the G/On update CD Button. *This option is presented by a Mouse Right Click on the G/On Icon*. If updates are available, they will be asked to run G/Update.

In the case the user is running G/Update from the command prompt, please be aware that any windows open onto the USB key's Read/Only or Read/Write partition will cause G/Update to stop and issue an error message (see screenshot).



In this case please direct the user to close all open applications that point to the USB device and then press "Retry" for G/Update to finish successfully. Alternatively press "Abort" to stop the update process. Pressing "Ignore" will not solve the issue and only leads to

the error message being repeated.

1. **Click “Yes” to start the update**
2. **Depending on whether or not you want to backup files, click either “Yes” or “No” to continue the update**

Note: This is the last chance to abort.

3. **Click “Yes” if you want to continue the update**
4. **Click “Yes” if you want the Read/Write partition updated with the software you have placed in the clients RWData directory on the G/On Server**
5. **Click “Yes” to continue the update, and the following dialogs will appear**

Note: This part of the update process may take several minutes, but as long as the LED on the G/On USB Key is blinking, the update process is still in progress.

6. **Press “OK” to finish the update process.**
7. **When the update process has completed, the dialog above appears. Simply close the G/On**

To see a complete list of all supported switches in G/Update, start G/Update with the “/?” switch

(“GUpdate.exe /?”), this will produce the help screen.

Name of Switch	Description	Can be used with these Switches
/deploy	The **/deploy** switch is not case sensitive with the name of the ISO image file, nor does it require the ".iso" extension on the name of the image. This feature **DOES NOT** import current files from the Read/Only partition of the G/On USB Key.	/deploy is not compatible with other switches and should be used alone.
/getall	switch changes the default mode of operation, so G/Update updates all current files and downloads all files that are not present on the USB key.	Compatible with /updaterw /ignorecrc /updateonly /updaterw
/updaterw	toggles G/Update to update the Read/Write partition on the G/On USB Key with the contents of the **\RWData** folder under the EMCADS installation folder. ***Note: please always launch with /getall to ensure proper updating of Read/Write partition***	Compatible with /getall /updateonly /ignorecrc /no import
/updateonly	instructs G/Update to limit updating to either a folder (and its subfolders) or a single file. For example: Invoking G/Update with the following parameters **GUpdate.exe /updaterw /updateonly wfica\appsrv.ini** will update the appsrv.ini file in the wfica folder. However, invoking G/Update with the following parameters **GUpdate.exe /updaterw /updateonly wfica** will update the entire wfica	Compatible with /getall /updaterw /ignorecrc /noimport

	folder. The trailing \ (backslash) in the "wfica\" is what tells G/Update if it's a folder or a file it should attempt to update.	
/noimport	The /noimport switch tells G/Update to ignore what is already present on the part of the G/On USB Key or G/On Desktop it's about to update. This means it will not import files currently on the Read/Only partition, even if they were NOT the latest version. However, on the Read/Write drive partition of the G/On USB Key or G/On Desktop "Applications" Directory it will delete all files present before downloading the updates, effectively achieving the same as with the Read/Only partition.	/getall /updateonly /updaterw /ignorecrc
/ignorecrc	will cause it to only download a fresh copy of all files currently present, i.e. it will not download files that do not already exist on the G/On USB Key.	/getall /noimport /updaterw /updateonly
/autoclose	This switch will make GUpdate automatically close itself, when finished (if no errors occurred during the run)	Can be used with all the other switches except /nukethekey
/nukethekey	This is a special switch that changes the behavior of G/Update. It should be used with **great care**. because using this switch resets all other switches either to predefined values, or ignores them. It also disables user intervention and defaults actions to "yes" on all dialogs except the "Safety backup" dialog. ***Note: All files currently on the Read/Write drive partition will be destroyed when this switch***	Not compatible with other switches. Only available for USB Key.

	is used. This option is designed to deploy - or re-deploy - a user with the minimum of user intervention. This option will download all files currently in the root of the .**\Clients** folder (same as **/getall** and **/ignorecrc**), ignore the current content (same as **/noimport**), record the image and run one more time to update the Read/Write drive partition on the G/On USB Key (same as **/updaterw**). **NOTE:** It is NOT possible for the user to abort the application before both the Read/Only and Read/Write drive partition are updated. The only emergency last-resort options are to either kill the G/Update (process in Windows Task manager or physically remove the G/On USB Key before G/Update starts recording to the Read/Only partition.	
/nodialog	This switch will suppress status dialogs except error messages.	Can be used with all other switches.
/launchgon	This switch will launch the G/On client when Gupdate exits	Can be used with all other switches except /Nukethekey
/yestoall	This switch will cause G/Update to automatically respond yes to all following popup windows	

Note:

/nukethekey is not available on G/On Desktop Clients.

Chapter

11

System Backup & Restore

Backup and Restore is a Key feature of any software installation. For G/On there are two groups of critical settings that you should backup and store in a safe location.

Every company has their own policies for how often they should back up data and on safe storage. In order to ensure that your G/On installation remains secure and save from server failure, upgrade error or other potential disasters, we recommend that you backup your system before and after any installation and after making any major changes to your applications or user groups.

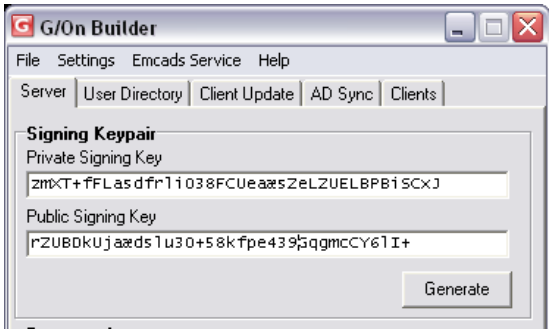
There are two primary items to backup in your G/On Installation:

Copy your Signing KeyPair

Backup your Database

Signing Keypair Backup

The **Signing Keypair** is the private and public keys that the G/On Server uses to identify its clients and vice-versa.



- **Copy both the Private and the Public Signing Keypair to a text file and store the file in a secure location.**

Warning: Generating Signing Keypairs

Never use the "Generate" Button on a running system, unless you plan to redeploy new USB keys and Desktop Clients to all users. Generating a Signing Keypair should only be done on NEW INSTALLATIONS as all deployed keys will cease to work, as they no longer "share a secret" with the server (the identity file is wrong). To redeploy, you need to distribute a new identity file. *Please keep copies of the keys in a safe and secured place as they are an integrated part of the mutual authentication process*

Copyright Giritech A/S 2009

G/On Backup /Restore

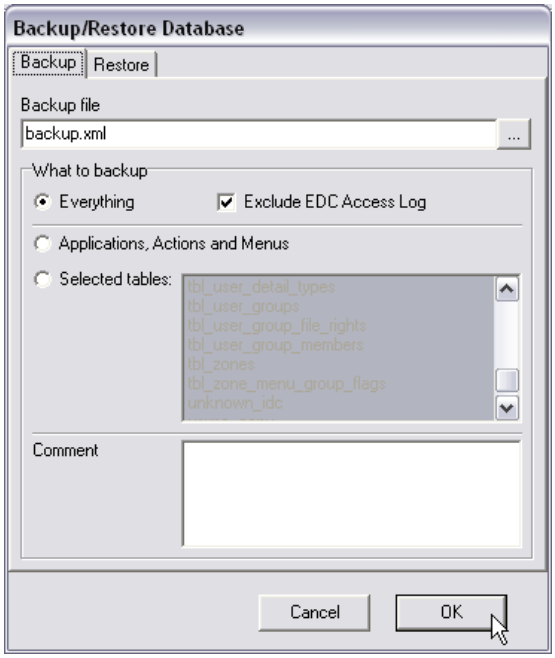
G/On Admin lets you perform database backups to .xml files, and later restore them. Fill in a path and name for the file you want to backup to and check the relevant settings:

"Everything" includes literally everything in your database, with the option to exclude the EDC access log.

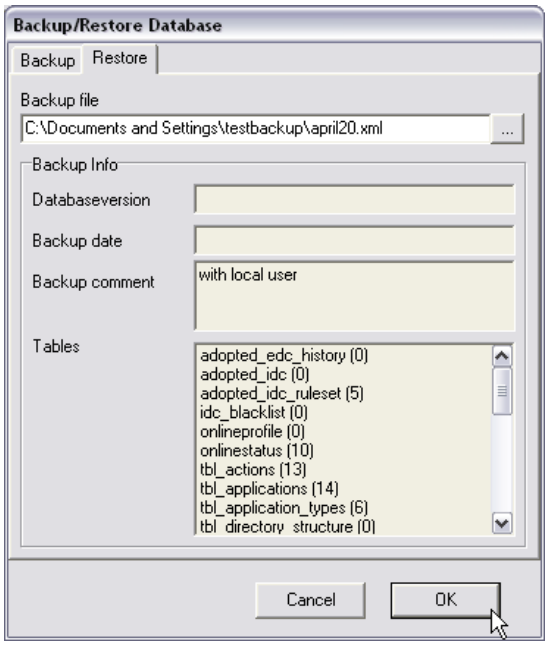
"Applications, Actions and Menus": This option covers information in the database, which produces the data in the first three tabs in G/On Admin. This gives you the option to save your setup with no users. Note, that menu association to groups/users will be lost if you later restore this kind of backup.

"Selected tables": This option enables you to backup only certain tables of your own choice from the database.

In the comment field, you can type information about the backup, at your own convenience.



NOTE: .xml files from a backup operation are not encrypted, whether you are using an encrypted database or not.



G/On Restore

The restore tab is where you restore .xml backup files to your database.

When an .xml file is chosen for restoring, the fields in the restore view will provide you with information about the particular file.

Click on "OK" to restore the file after an overwrite warning.

Copyright Giritech A/S 2009

Chapter

12

Overview of Application Connectivity

Examples for creating connectivity to the most common application types are covered in Chapter 6. This chapter is meant to provide a foundation for companies understand the basic structure of application connectivity and to enable them to configure other applications.

To implement a connection to an application using G/On, you need to understand how the application communicates over a network. We recommend all administrators of this functionality to contact Giritech for details on a coming training course in “Advanced Application Connectivity”

With Client/Server applications working on TCP/IP, the client application typically connects to the server application by connecting to the server’s IP address or name on one or more port/s.

G/On addresses all Client/Server applications that connect to a fixed IP number (or DNS name), on fixed ports.

G/On supports TCP and UDP connections.

To implement a connection to an application using G/On, you need to understand how the application communicates over the network. Typically a client connects to a server using specific ports and protocols.

To find out how an application communicates, refer to the application documentation, proxy or firewall configuration, netstat.exe or a network communication program like CommView: http://www.tamos.com/products/commview/ which can be used to analyze the communication between the client and the server.

Application Guidance

Some applications do not natively run on fixed ports (EMAP - Ephemeral Port Mapping) but can be modified to do so.

Some Client applications consist of only one, executable file. An example GGW.exe;

To start an application from a G/On menu, the full path to the local executable needs to be included in the application string: i.e. C:\Program Files\Microsoft Office\Office11\Outlook.exe

Understanding what ports the application uses to communicate with its server, will make connecting with the G/on Client a straightforward process.

Note: Looking in the firewall section of the GGW Administrator's guide provides the information of the port the GGW uses to Communicate over the Network:

Applications Running Multiple Executables

Other client applications are suites of executables, accompanying .dll and .ocx files, and it may be difficult to identify the executable that actually makes the outgoing connection from the client PC.

You can set up a G/On gateway that will permit different applications on the client PC to connect through the G/On Gateway connection ("Lock to process" turned off).

i.e. CITRIX communicates on 1494 TCP, 1604 UDP and 2598 TCP. The following Citrix applications use one or all of the ports: Wfcrun32.exe = 1494, PN.exe = 1494 + 1604 or 2598

G/On Communication

The G/On connection communicates on the loopback IP 127.0.0.2.

Most client applications can be configured to communicate on the loopback address. This is normally done with a command line switch or is configured in the application.

In the Citrix application, PN.exe is configured using APPSRV.ini where you point the client to the firewall connection of 127.0.0.2 instead of the true server location. Wfcrun32.exe is configured on the command line or by using an application specific ica file.

Note:

Some applications require "split DNS". Please refer to the Split DNS whitepaper for more information.

Note:

At certain times, even a windows command line is not enough to launch a specific client application correctly. You can be forced into launching a script/batch file instead.

To launch a .cmd or .bat file with G/On, make your "Application to launch":

%WINSYSDIR,noedit%\cmd.exe

and the "Application Parameters":

/C PathTo\MyScript.bat

Example: you would like to launch "startprog.bat"; a batch file residing in a directory called "batch" in

the root of the Read/Write partition of a G/On USB key

Application to launch: %WINSYSDIR,noedit%\cmd.exe

Application parameters: /C %VENDORPATH,noedit%\batch\startprog.bat

You can not launch the startprog.bat simply by using its name as a windows command.

Likewise, it is not possible to launch, for example, an MS Word document by invoking its full path and name. Instead, you must start Winword.exe (with full path), and as a parameter, put in full path to the document.

An example of this could be:

Fixed Path

Application to Launch "C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE"

Application parameters: %VENDORPATH,noedit%\MyDocument.doc

However, this would only launch MS Word on an English Windows with Office 2003 installed. Application to launch:

Using the Registry Paths

!HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AppPaths\Winword.exe\Path! (notice, there is a space in "App Paths" where the line breaks)

Application parameters: %VENDORPATH,noedit%\MyDocument.doc

This string will work on any language version of Windows, and with any version of MSOffice.

Chapter

13

Introduction to HTTP proxy support

HTTP proxies are servers setup between the internal network (the LAN) and the Internet. HTTP proxies often have many purposes but one of them is to block all traffic that is not standard web traffic (HTTP). From a HTTP proxy "protected" foreign network, standard G/On TCP traffic will not be allowed to leave the foreign network and the G/On connection attempt will fail.

Giritech ToH (TCP over HTTP) is a support tool to G/On 3.4, 3.5 and 3.6 that address this problem of a G/On client being a guest on a foreign network where connections directly to the G/On server is blocked, and the only access to the internet is through an HTTP proxy. I.e. when trying to connect from within a foreign network that is not under the G/On Admin's control.

In this scenario, a G/On Administrator can enable ToH for *his* clients and on *his* server, and thus enable his clients to connect through foreign HTTP proxies, through the untrusted internet and through his ToH server to his G/On server

Note:

G/On HTTP proxy bypass is a command prompt based tool that requires a deep understanding of Windows and Internet configurations. Installation and configuration are therefore only recommended for advanced G/On users. Please contact Giritech Support for help.

Security Warning:

Connecting through an HTTP proxy might be a violation of local security policies as the proxy is typically implemented to control and prevent users accessing the Internet.

Introduction to the HTTP proxy tool

The Giritech "TCP over http" tool, ToH establish an additional network "layer" that:

1. On client side (ToH client) encapsulate the normal G/On traffic in HTTP and communicates this via the client side HTTP proxy as standard web traffic that will therefore forward the traffic to the Internet targeting a ToH server

2. On server side (ToH server) will receive that traffic, as HTTP web traffic, de-capsulate into normal G/On traffic and forward to the G/On server

The “ToH layer” is thus transparent to the G/On client and server and the client side HTTP proxy server will likewise not be aware of the G/On client to G/On server communication.

Note:

Due to the inevitable overhead associated with HTTP tunneling using HTTP proxy support will affect performance negatively (higher latency and lower effective bandwidth).

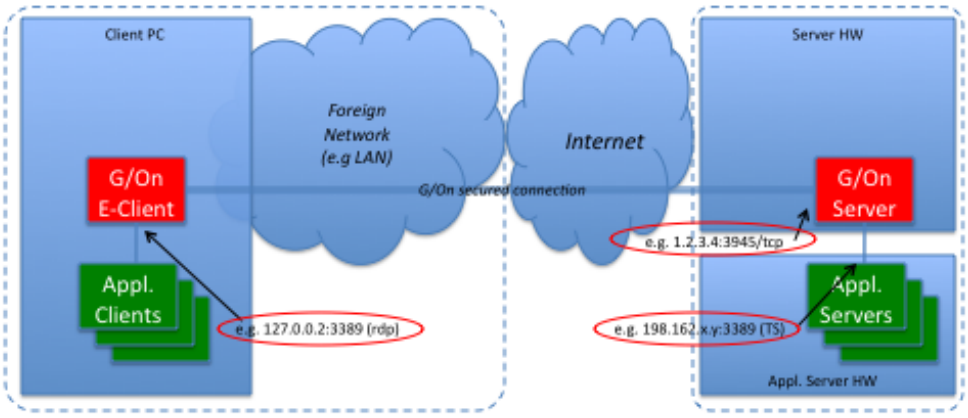
Note:

G/Update will not run through the HTTP Proxy tool!

The overall architecture of the problem and the components of the solution can be found on the following figures, 1st the default G/On setup without proxy:

1

Standard G/On configuration
(no client side proxy – hence no ToH needed)

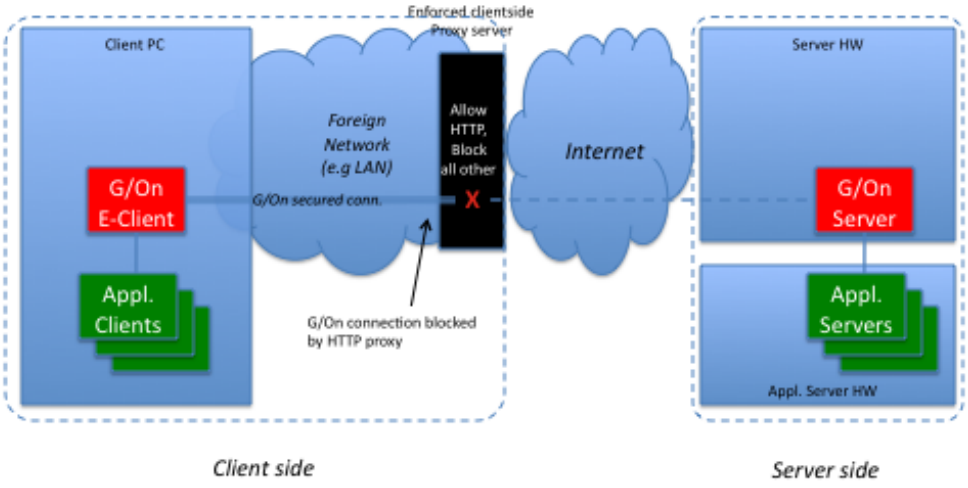


Please note that routers, firewalls and DMZs are not shown on this figure. Please consult other Giritech documentation

Then introducing an HTTP proxy at the client side in the same foreign network as above and thus blocking the direct G/On client to G/On server traffic:

2

When a client side HTTP Proxy is inserted
G/On traffic blocked

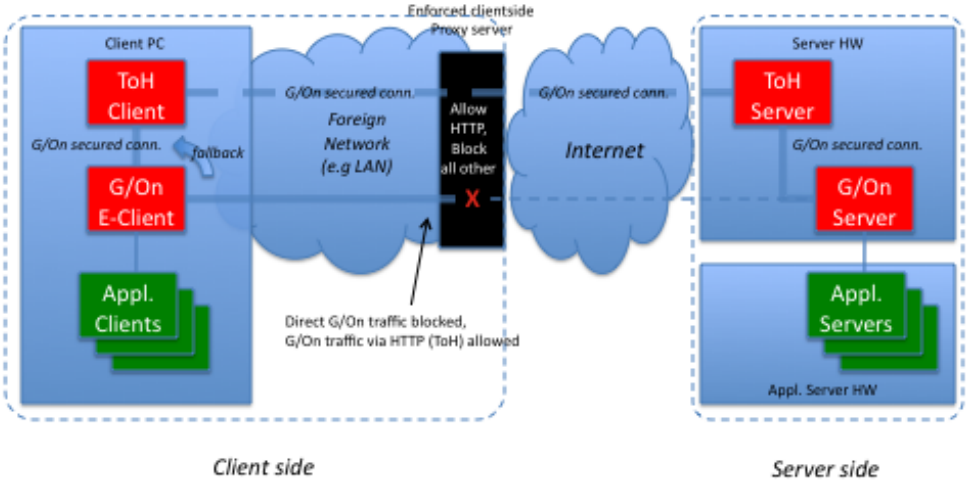


Please note that routers, firewalls and DMZs are not shown on this figure. Please consult other Giritech documentation

Then setting up the ToH network layer to support connectivity via the HTTP proxy:

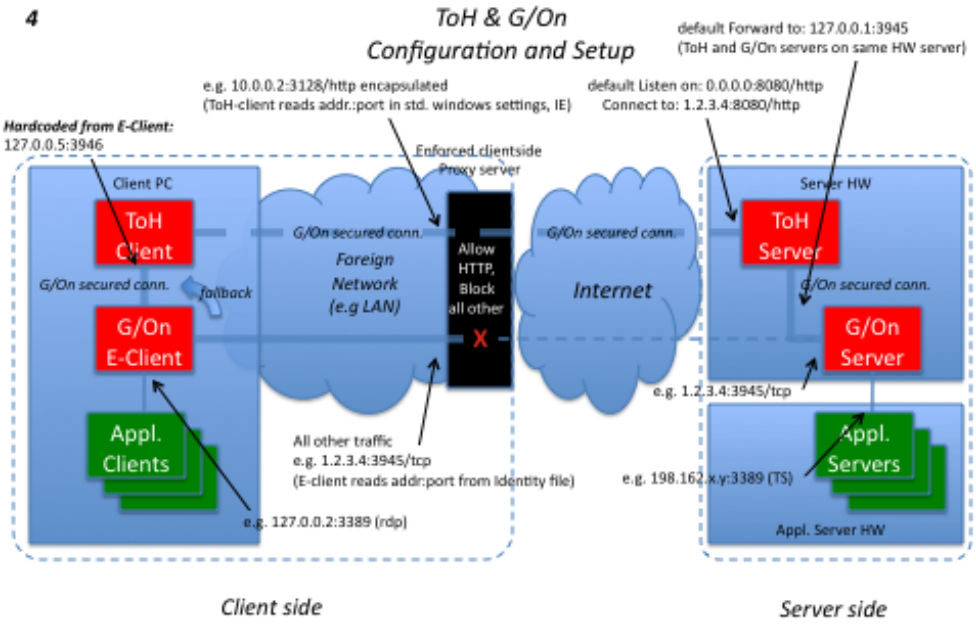
3

Inserting ToH:
Re-establishing the G/On connection



Please note that routers, firewalls and DMZs are not shown on this figure. Please consult other Giritech documentation

The next slide explains the individual addresses involved in the establishment of a ToH layer:



Please note that routers, firewalls and DMZs are not shown on this figure. Please consult other Giritech documentation

Analysing the network

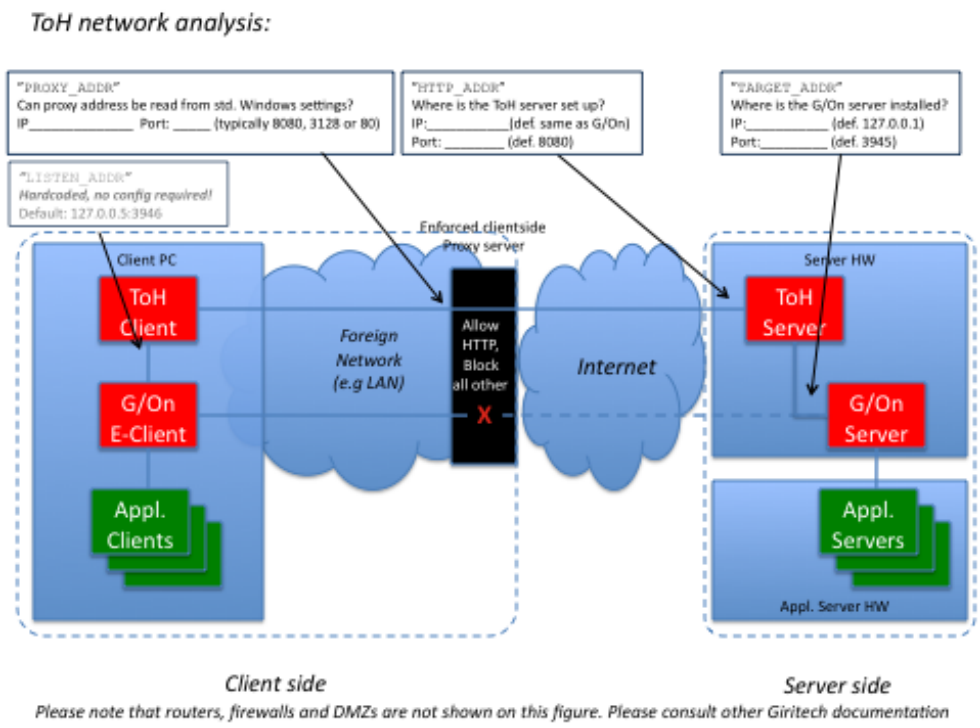
So to perform a ToH installation and setup a series of steps have to be performed:

- Analysis
  - Critical first step uncovering all the necessary network data required for correct ToH configuration.
  - See the following supporting slide (“ToH network analysis”)
- Configuration
  - Setting up the configuration: G/On Builder (clients) and ToH server
  - Testing the configuration
- Launching
  - Ensuring that the setup remains operational (installing and starting the correct services)

The following slide (“ToH Network Analysis”) summarize the network data that needs to be collected to properly configure a ToH setup.

It is based on, and assumes understanding of, the architecture drawing and terminology described in the previous sections:

Copyright Giritech A/S 2009



ToH addresses in the ToH-client and ToH-server .ini files as outlined on above slide:

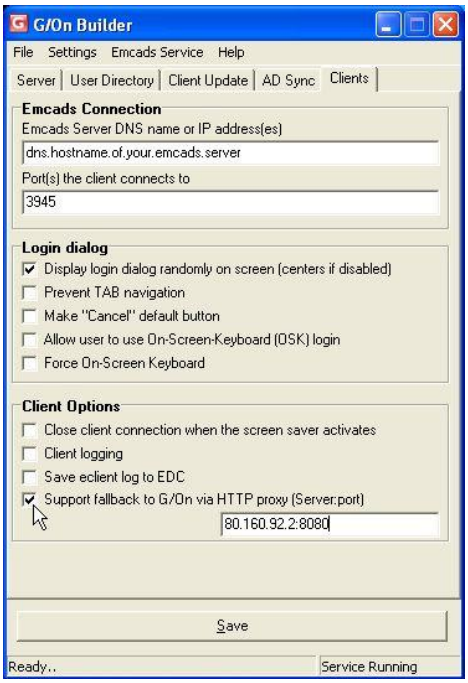
- `LISTEN_ADDR`: the IP address (and port) where the ToH client will listen for traffic from E-client. This address is provided by E-client so any changes to ToH-client.ini will be overruled by E-client. Note that E-client uses a hardcoded address (127.0.0.5:3946)
- `PROXY_ADDR`: the IP address (and port) of the client side HTTP Proxy server on the foreign network. This address will default be found by the ToH-client via the windows (IE) settings on the client side computer when connected to the foreign network.
- `HTTP_ADDR`: the external target IP address (and port) of the ToH-server that the ToH-client should request the client side Proxy server to connect to. Default settings are the same IP address as the G/On server but on port 8080. The address is provided by E-client when it starts the ToH-client and originates from the Identity file. Note that the ToH-server will default listen on port 8080 on all IP addresses (IP address 0.0.0.0)
- `TARGET_ADDR`: The IP address (and port) of the G/On server where the ToH-server will deliver the traffic from ToH-clients. Default setting is 127.0.0.1:3945 assuming that the G/On and ToH-servers are 1. running on the same physical server and 2. the G/On server listens on port 3945 (the default listen port of a G/On server)

Copyright Giritech A/S 2009

Setting up and Configuring ToH with G/On

To setup ToH in G/On there is only one setting required: "**Support fallback to G/On via HTTP proxy**"

This address is entered in G/On Builder (as shown on the figure) and is the target address of the ToH server (`HTTP_ADDR`). Typically the same IP address as the G/On server itself but using port 8080 instead of the typical default G/Onport 3945.



- **Remember to press "Save", no restart of G/On server (Emcads service) required**
- **Distribute the new Identity file to all users (as always when making changes in the Builder Client tab)**
- **Restart G/On clients**

Afterwards the ToH server must be installed as a service from the command line in the Emcads directory:

- "ToH-server.exe install"
- Check via Windows Services Control Panel: "Start->Control Panel->Administrative tools->Service" look for "Giritech ToH"

To remove the ToH server, enter: "ToH-server.exe remove" from the Emcads directory on the command line.

All settings will be automatically read from "ToH-server.ini" as described previously.

This will install the ToH-server as a service together with the G/On server (provided they run on the same server hardware which is the recommended standard setup).

Note:

For testing the bypass server can be started manually in a DOS window on the server machine. In production settings it should be launched and running as a service on the bypass server

Note:

Logging and logging levels (higher means more information) can be enabled on both server and client side by enabling the "`LOG_FILENAME`" and "`LOG_LEVEL`" parameters in the .ini files. "`#`" in front of an item means that the item has been disabled (commented out) in the .ini file.

This concludes the setup and configuration of ToH. When operational the ToH solution works as follows:

E-client launches ToH *only upon fallback when direct connection attempts fail* with command line parameters:

- `toh-client.exe --HTTP_ADDR=80.160.92.2:8080 --LISTEN_ADDR=127.0.0.5:3946 --MAX_IDLE_SESSION=5`

E-client waits approx. 5 seconds and then starts communicating with ToH-client

`HTTP_ADDR` is read from the G/On builder settings:

- Builder->Clients->Client options->"Support fallback to G/On via HTTP proxy" (see screenshot)
- In the example above: 80.160.92.2:8080

`LISTEN_ADDR` is hardcoded in E-client:

- 127.0.0.5:3946

Note:

G/ON Builder does not change any of the .ini settings but the commandline parameters will overrule the .ini settings.

Note:

The use of ToH does not change any G/On server settings or function.

Warning:

The When using ToH fallback it is recommended not to try ports 80 or 443 as part of the normal range of IP:ports! Otherwise some proxies might create a false response to G/On and hence G/On will never actually fallback to ToH.

Standard recommended configuration:

<G/On server IP address>:3945, ToH

Not recommended:

G/IP:3945, G/IP:443, G/IP:80, ToH

See G/On Builder->Clients->Emcads Connection.

Warning:

ToH supports HTTP proxies. In cases where deep packet inspection firewalls are used, ToH can not provide the expected connectivity

Compliance and tested proxies

The G/On HTTP Proxy bypass tool has been designed to work wth HTTP 1.0 and 1.1 and comply with RFC 1945, 2068 and 2616. The tool have been tested with:

- Squid (http://www.squid-cache.org/)
- Microsoft ISA (http://www.microsoft.com/isaserver/default.mspx)
- JanaServer2 (http://www.janaserver.de/start.php?lang=en)